Komparativna analiza antivirusnih alata operativnih sustava Android i iOS

Pejić, Tomislav

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:885893

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Tomislav Pejić

Komparativna analiza antivirusnih alata operativnih sustava Android i iOS

DIPLOMSKI RAD

Zagreb, 2015.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

Komparativna analiza antivirusnih alata operativnih sustava Android i iOS

Comparative analysis of antivirus tools for Android and iOS operating systems

Mentor:
izv. prof. dr. sc. Dragan Peraković

Student: Tomislav Pejić
JMBAG: 0135213434

Zagreb, 2015.

SADRŽAJ:

1. Uvod ... 1
2. Razvoj i korištenje mobilnih terminalnih uređaja ... 3
   2.1. Razvoj mobilnih terminalnih uređaja ... 3
   2.2. Korištenje mobilnih terminalnih uređaja ... 8
3. Arhitektura Android i iOS operativnih sustava ... 10
   3.1. Android operativni sustav ... 10
   3.2. iOS operativni sustav ... 12
4. Sigurnosne prijetnje mobilnih terminalnih uređaja ... 14
   4.1. Aplikacijski-bazirane prijetnje ... 14
   4.2. Web-bazirane prijetnje ... 15
   4.3. Mrežno bazirane prijetnje ... 15
   4.4. Fizičke prijetnje ... 16
5. Antivirusni alati ... 17
   5.1. Lookout ... 17
      5.1.1. Podešavanje Lookout aplikacije ... 18
      5.1.2. Funkcionalnosti Lookout aplikacije ... 19
      5.1.3. Otkrivanje sigurnosnih prijetnji i performanse ... 24
   5.2. Avast Mobile Security ... 24
      5.2.1. Podešavanje Avast aplikacije ... 24
      5.2.2. Funkcionalnosti Avast aplikacije ... 25
      5.2.3. Otkrivanje sigurnosnih prijetnji i performanse ... 29
   5.3. Trend Micro Mobile Security ... 29
      5.3.1. Podešavanje Trend Micro aplikacije ... 31
      5.3.2. Funkcionalnosti Trend Micro aplikacije ... 31
      5.3.3. Otkrivanje sigurnosnih prijetnji i performanse ... 36
   5.4. McAfee Mobile Security ... 36
      5.4.1. Podešavanje Mcafee aplikacije ... 37
      5.4.2. Funkcionalnosti Mcafee aplikacije ... 38
      5.4.3. Otkrivanje sigurnosnih prijetnji i performanse ... 42
   5.5. Norton Mobile Security ... 42
      5.5.1. Podešavanje Norton Mobile Security aplikacije ... 43
      5.5.2. Funkcionalnosti Norton Mobile Security aplikacije ... 44
      5.5.3. Otkrivanje sigurnosnih prijetnji i performanse ... 47
6. Komparativna analiza antivirusnih alata ... 47
   5.2. Korišteni mobilni terminalni uređaji ... 47
   5.3. EICAR test ... 49
   5.4. Najposjećenije Web stranice u Hrvatskoj ... 51
   5.5. Testiranje uzorcima malware-a ... 53
   5.6. Statistička analiza rezultata ... 57
7. Zaključak ... 59

Literatura 61
Popis slika 63
Popis tablica 65

Sažetak

Cilj rada je usporedba 5 antivirusnih alata na Android operativnom sustavu sa 1 antivirusnim alatom na iOS operativnom sustavu. Cilj je utvrditi razlike između antivirusnih alata kod pronalaska zlonamjernog sadržaja te ih statistički obraditi. Također cilj je upozoriti korisnike na moguće prijetnje kod korištenja mobilnih terminalnih uređaja, istaknuti značajke Android i iOS operativnog sustava. Svrha istraživanja je dati korisnicima mobilnih terminalnih uređaja uvid u pojedine antivirusne alate. Za testiranje antivirusnih alata koristit će se EICAR testna datoteka, uzorci virusa te će se ispitat sigurnost pedeset najposjećenijih web stranica u Hrvatskoj. Rezultati će dati korisnicima uvid u potencijalne prijetnje, razinu zaštite koju nude antivirusni alati i efikasnost istih.

KLJUČNE RIJEČI: antivirusni alati; Android; iOS; komparativna analiza; mobilni terminalni uređaj; virus;

Summary

The aim was to compare five antivirus tools on the Android operating system with one anti-virus tool on iOS operating system. The goal is to determine the differences between the antivirus tools in finding malicious content and statistically processed them. It is intended to alert users to possible threats in the use of mobile terminal devices, highlight features of Android and iOS operating systems. The purpose of the research is to provide users of mobile terminal devices insights into to certain antivirus tools. To test antivirus tools will be used EICAR test file, virus samples, and will examine the safety of the fifty most visited websites in Croatia. The results will give users insight into the potential threats, the protection offered by anti-virus tools and effectiveness.

KEYWORDS: antivirus tools; Android; iOS, mobile terminal device; comparative analysis; malware;

1. Uvod

Sigurnost mobilnih uređaja postaje sve više aktualna tema. Broj mobilnih terminalnih uređaja je nadmašio ukupnu svjetsku populaciju 2014. godine. Mobilni terminalni uređaji brzo zamjenjuju osobna računala kod kuće i na radnom mjestu, prodaja mobilnih terminalnih uređaja je već nadmašila prodaju osobnih računala.

Zaštita mobilnih terminalnih uređaja je važan korak u zaštiti osobnih podataka korisnika ili podataka poduzeća. Zbog sve većeg oslanjanja korisnika na mobilne terminalne uređaje, veće su šanse napada na korisnikovu privatnost i njihove osobne podatke.

Današnji napredni mobilni terminalni uređaji koje još nazivamo pametni telefoni (*smartphone*) dobro su povezani s internetom i imaju daleko više mogućnosti nego mobilni terminalni uređaji u prošlosti. Koriste se kao osobna računala što ih čini potencijalno osjetljivim na slične prijetnje koje se pojavljuju kod osobnih računala. Budući da mobilni terminalni uređaji mogu sadržavati velike količine osjetljivih i osobnih podataka privlačne su mete koje pružaju jedinstvene mogućnosti za kriminalce u namjeri da ih iskoriste.

U prošlosti su zlonamjerne aktivnosti ciljane prema mobilnim terminalnim uređajima bile ograničene u usporedbi s računalima. Razlozi su bili ograničene funkcionalnosti arhitekture hardvera i softvera. Današnji mobilni terminalni uređaji imaju mnogo veće funkcionalnosti i dostupniju arhitekturu što je rezultiralo povećanjem zlonamjernih aktivnosti.

Svrha istraživanja je dati korisnicima mobilnih terminalnih uređaja uvid u pojedine antivirusne alate, njihove prednosti i nedostatke, te prikazati točnost kod pronalaženja zlonamjernog sadržaja.

Cilj rada je usporedba 5 antivirusnih alata na Android operativnom sustavu sa 1 antivirusnim alatom na iOS operativnom sustavu. Cilj je istražiti koje internet stranice su najrizičnije za pretraživanje. Cilj je utvrditi razlike između antivirusnih alata kod pronalaska zlonamjernog sadržaja te ih statistički obraditi. Cilj je istražiti hoće li svi antivirusni alati upozoriti korisnika na zlonamjerni sadržaj ili će ga upozoriti i onda kada se ne radi o zlonamjernom sadržaju. Cilj je upozoriti korisnike na moguće prijetnje kod korištenja mobilnih terminalnih uređaja, istaknuti značajke Android i iOS operativnog sustava.

Diplomski rad se sastoji od sedam funkcionalno povezanih poglavlja koja su ukratko opisana u nastavku.

1. Uvod
2. Razvoj i korištenje mobilnih terminalnih uređaja
3. Arhitektura Android i iOS operativnih sustava
4. Sigurnosne prijetnje mobilnih terminalnih uređaja
5. Antivirusni alati
6. Komparativna analiza antivirusnih alata
7. Zaključak

U drugom poglavlju je opisan razvoj mobilnih terminalnih uređaja kroz povijest od samih početaka pa sve do današnjih pametnih telefona, te korištenje samih uređaja i statistike vezane uz njih. Također su opisani i sustavi pokretne telefonije po generacijama.

Treće poglavlje daje osnovni uvid u arhitekturu operativnih sustava Android i iOS, sustava koji će se pokretati na mobilnim terminalnim uređajima na kojima će biti instalirani antivirusni alati te na kojima će se raditi istraživanje.

U četvrtom poglavlju biti će opisane kategorije sigurnosnih prijetnji mobilnih terminalnih uređaja.

Antivirusni alati koji će se koristiti u diplomskom radu biti će opisani u petom poglavlju.

Praktični dio istraživanja biti će opisan u šestom poglavlju, te će biti prikazana komparativna analiza antivirusnih alata koji su se koristili u istraživanju.

U posljednjem poglavlju, Zaključku, sintetizirane su sve informacije prikupljene i obrađene tijekom izrade diplomskog rada.

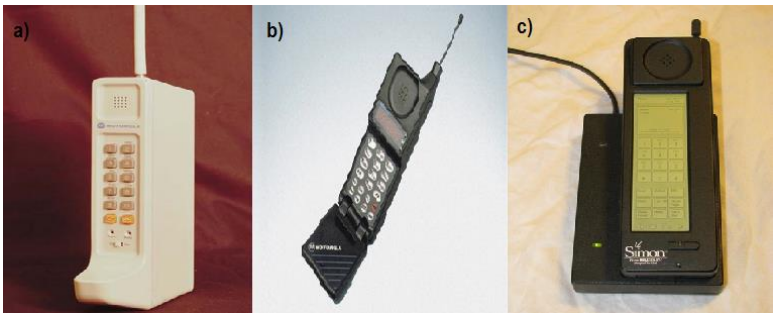
2. Razvoj i korištenje mobilnih terminalnih uređaja

Naziv terminala potječe od činjenice, da je njegova veza do centrale djelomično realizirana sa bežičnom (radio) vezom, pa ga se može koristiti i u kretanju. Za razliku od telefona bez vrpce koji je također bežičan na dijelu veze, pomoću pokretnog telefona moguće je ostvariti telefonsku vezu na znatno većoj udaljenosti od temeljne radio postaje, [1].

2.1. Razvoj mobilnih terminalnih uređaja

Telefoni temeljeni na radio tehnologiji imaju dugu povijest i datiraju još od izuma Reginalda Fessendena, koji je omogućio komunikaciju broda s obalom korištenjem radio telefonije. Tokom Drugog svjetskog rata vojska je koristila mobilne radijske uređaje za komunikaciju. U pedesetim godinama 20. stoljeća ista se tehnologija prilagodila civilnoj upotrebi (npr. policija, taxi vozila i slično), [2].

Izum mobilnih telefona koji su slični današnjim uređajima pripisuje se Martinu Cooperu, zaposleniku i istraživaču tvrtke Motorola. On je u početku razvijao ćelijski telefon (mobitel) nazvan Motorola Dynatac 1973. godine. Širine 12.7 cm i 22.9 cm duljine koji je težio oko 1.1 kg i u sebi je je imao oko 30 sklopovskih pločica. Punjenje je trajalo oko 10 sati, a vrijeme razgovora 35 minuta koje je korisniku pružalo ugodno iskustvo razgovora. Korisnik je mogao slušati, birati i razgovarati ali ono što je nedostajalo bio je zaslon. S vremenom su napravljena poboljšanja uređaja. Potrebno je napomenuti kako je postojala duga utrka između Motorole i Bell Labs-a tko će prvi izumiti moderni mobilni telefon. Cooper je uputio prvi poziv upotrebom mobitela svojem suparniku Joelu S. Engelu u Bell Labsu, [3]. Na slici 2.1 a) prikazan je prvi mobilni telefon.



Slika 2.1. a) Motorola DynaTAC, [4] b) Motorola MicroTA, [5] C c) IBM Simon, [6]

1989. godine Motorola je napravila prvi preklopni mobilni telefon koji se zvao Motorola MicroTAC. Hardver je bio smješten u preklopnom dijelu mobitela smanjujući tako veličinu uređaja kada se nije bio u uporabi. To je bio prvi džepni mobitel, [5].

Desetljeće nakon što je Martin Cooper napravio prvi poziv, američki FCC (Federal Communications Commission) je odobrio Motorolu DynaTAC za javnu upotrebu. Godine 1984. DynaTAC je postao dostupan za potrošače. Mobilni uređaj je težio 0.8 kg, a njegova punjiva baterija je trajala 8h prema izvješću tvrtke iz 1970. godine. U priopćenju, tvrtka je izjavila da vjeruje da će ljudi nastaviti koristiti svoje telefone u automobilima, te da mobiteli apsolutno neće zamijeniti standardne telefone, [6].

Godine 1993. Bellsouth i IBM[1] su najavili stvaranje Simon-a, telefona kao osobnog komunikatora, krišom promatranog kao prvog smartphone-a u svijetu. Primarna zadaća Simon-a je bila da bude mobitel, a sekundarna da bude računalo, tako se predstavljalo u medijima. Preporučena cijena uređaja je bila 899$ te je imao sljedeće značajke:

- *Pager*,
- *e-mail*,
- *stylus* za pisanje po zaslonu,
- potpuna tipkovnica koja sadrži slova i brojeve,
- kalendar koji se može automatski ažurirati s udaljenog računala.

Napravljeno samo 2000 uređaja koji su težili nešto manje od 0.5 kg

Sharp je 2000. godine napravio prvi mobitel sa kamerom, model je bio J-SH04 (J-Phone), objavio ga je J-Mobile u Japanu. Nudio je kameru razlučivosti 0.1 megapiksela.

Slika 2.2. Sharp J-SH04 i fotografija snimljen njegovom kamerom, [7], [8]

Motorola RAZR je bio među prvim mobilnim telefonima koji se prodavao kao „modni“ telefon, te se sve više počela pridonositi pažnja dizajnu mobilnih uređaja. U četiri godine

[1] IBM-International Business Machines

razvoja prodaj je u više od 130 milijuna primjeraka te je bio najprodavaniji preklopni mobilni telefon. Slika 2.3. prikazuje Motorolu RAZR.

Slika 2.3. Motorola RAZR, [5]

U 2007. godini, Steve Jobs je predstavio Apple iPhone, revolucionarni smartphone sa zaslonom na dodir. To nije bio prvi smartphone, ali je bio prvi koji je dobio pravo korisničko sučelje, kasnije prilagođen 3G tehnologiji (koja je bila dostupna od 2001. godine).

Slika 2.4. Apple iPhone, [5]

Prvi smartphone na kojem je pokrenut Google-ov Android operativni sustav bio je HTC Dream klizni telefon.

Slika 2.5. HTC Dream, [5]

Imao je QWERTY tipkovnicu, potpuni HTML[2] web preglednik, Gmail, Youtube i još mnogo toga i otvorio je put telefonima kao što su Nexus One i Motorola Drodi.

[2] HTML-HyperText Markup Language

HTC EVO 4G je bio prvi mobilni telefon koji je podržavao 4G standard, pokrenut na WiMAX[3] mreži. Prodavao se sa Android sustavom 2.1 te je imao jedno od najvećih zaslona na dodir, kameru od 8 MP, HD video snimanje, HDMI izlaz, mogućnost dijeljenja mobilne mreže i HTC Sense.

Slika 2.6. HTC EVO 4G, [5]

Povijest mobilnih telefona se dogodila kroz relativno kratko vrijeme, ali razvoj ćelijskih tehnologija se razvija ogromnim koracima. Kao oblik dvosmjerne radio komunikacije, ćelijska tehnologija je nadmašila sve ostale oblike radio komunikacijskih tehnologija. Bilo je potrebno tek nešto više od 20 godina da se migrira sa analognih sustava na 3G sustave koji su u stanu prenositi podatke velikim brzinama. Brzim razvojem tehnologije počeo se koristiti 4G sustav, a daljnjim razvojem se predviđa korištenje 5G sustava do 2025. godine, [9].

Sustavi pokretne telefonije obično se dijele po generacijama.

Generacije pokretne telefonije:

1) **1G prva generacija -** Komunikacijski čvorovi omogućavali su 'prebacivanje' iz jednog geografskog područja u drugo bez potrebe promjene radne frekvencije i svi su bili povezani s PTT[4] sustavom. Prvu komercijalnu automatiziranu mrežu čvorova ostvarila je tvrtka NTT (Nippon Telegraph and Telephone Corporation) 1979. godine, koja je koristeći 23 komunikacijska čvora 'pokrila' Tokio. Narednih pet godina NTT mreža je proširena duž cijelog Japana i postala je prva nacionalna 1G mreža u svijetu. Prijenos signala zasnivao se je na analognim tehnologijama. Sustav se bazira na FDMA koncepciji raspodjele kanala unutar zadanog frekventnog područja u rasponu od približno 800-900 MHZ, [10].

[3] WiMAX-Worldwide Interoperability for Microwave Access
[4] PTT-Postal Telegraph and Telephone

2) **2G druga generacija -** Devedesetih godina 20. stoljeća pojavila se druga generacija sustava mobilnih telefona koja je koristila GSM standard. Telefonski sustavi su se razlikovali od prethodne generacije u tome što su koristili digitalni prijenos podataka. U ovom su se razdoblju počeli koristiti pretplaćeni mobilni telefoni (*prepaid mobile phone*) za koje se kupuju bonovi koje će korisnik trošiti svaki puta kada nekome uputi poziv. Digitalni prijenos omogućava TDMA[5] raspodjelu kanala, a napredniji sustavi koristili su i CDMA raspodjelu kanala. Uvedeno je slanje poruka putem SMS-a (*Short Message Service*), u početku samo preko GSM[6] mreža, a kasnije i preko svih digitalnih mreža. SMS je ujedno prva usluga glede prijenosa podataka, uz osnovnu namjenu - razgovor. GSM je najpopularniji standard za sustave mobilne telefonije u svijetu. Jedna od ključnih značajki GSM mreže je SIM (*Subscriber Identity Module*) modul. SIM je pametna kartica koja sadrži podatke o korisnikovoj pretplati i telefonski imenik što omogućava korisniku da zadrži svoje podatke nakon promjene mobilnog uređaja. Frekventni opseg kojeg ovi uređaji koriste je 800-900 MHz ili 1800-1900 MHz, [10].

3) **3G treća generacija** - Odgovor je na sve veću potražnju za uslugama prijenosa podataka (kao što je Internet) i potrebu za većim brzinama prijenosa podataka. Koristi se nadograđeni CDMA[7] standard u uvodi se VoIP (*Voice over Internet Protocol*) tehnologija. Dakle, na osnovama TCP / IP skupu protokola što omogućava obavljanje telefonskog razgovora upotrebom postojećih mrežnih konekcija, kako u lokalnom i međugradskom prometu, tako i u međunarodnom. Velika prednost VoIP tehnologije je i mogućnost pozivanja mobilnih i fiksnih pretplatnika te ostvarivanje međunarodnih poziva po izuzetno povoljnim cijenama. Omogućene su brzine prijenosa podataka od 84 Mbit/s. Uređaji ove generacije koriste frekventni raspon približan 2G uređajima. Prvu nekomercijalnu mrežu pokrenula je tvrtka NTT[8] u Japanu na području Tokija 2001. godine, [10].

4) **4G četvrta generacija** - Do 2009. godine postalo je jasno da će 3G mreže postati preopterećene brojem korisnika i upotrebom aplikacija kojima je potreban širokopojasni kanal za prijenos podataka (kao što je na primjer prijenos multimedijskog toka podataka). Počeo je razvoj tehnologija koje su optimizirane za prijenos podataka i koje trebaju omogućiti prijenos podataka velikim brzinama (oko 10 puta brže nego

[5] TDMA-Time Division Multiple Access
[6] GSM-Global System for Mobile Communications
[7] CDMA-Code Division Multiple Access
[8] NTT-Nippon Telegraph and Telephone Corporation

3G). Prihvaćene tehnologije su WiMAX verzija za mobilne telefone i LTE (*Long-Term evolution*) standard koji razvija udruženje većine mobilnih operatera. Čvor kao pristupna komunikacijska točka „nestaje“ i koristi se IP mreža. Moderni uređaji ove generacije mogu biti ravnopravni članovi Wi-Fi (SOHO) mreže. OFDM (*Orthogonal Frequency-Division Multiplexing*) standard, sličan DVB-T[9] standardu, koristi se glede raspodjele kanala za prijenos podataka. Uređaji ove generacije koriste frekventni raspon kao 3G uređaji i raspon od približno 2500–2700 MHz. WiMax predviđa uporabu frekventnog područja od 3300-3800 MHz a u perspektivi i višeg. LTE[10] standard implementira kompatibilnost s prijašnjim standardima i to mu daje prednost u odnosu na WiMAX. Čini se da većina novih mobilnih operatera prihvaća LTE i da se ovaj nešto kasnije ustanovljen standard brže usvaja, [10].

2.2. Korištenje mobilnih terminalnih uređaja

Mobilni uređaji nisu više teški, sa malim ekranima i nepraktični te ne služe samo za pozive i slanje poruka. Današnji mobilni uređaji su postali mala računala i ne služe samo za telefonske pozive, već za snimanje, fotografiranje, slanje multimedijalnih sadržaja, surfanje Internetom i slično. Oni nude mogućnost pohrane i obrade podataka gotovo ekvivalentne osobnim računalima te pojedinci na njima mogu slagati materijale za učenje poput „lego kockica“. Prodaja mobilnih uređaja je nadmašila prodaju PC-a te njihova rastuća popularnost jasno određuje smjerove u kojima će se razvijati e-učenje u budućnosti. Na Tablici 2.1 možemo vidjeti porast prodaje mobilnih uređaja i tableta, a pad prodaje PC-a , [11].

Tablica 2.1.Prodaja mobilnih uređaja u odnosu na PC i tablet uređaje

Tip uređaja	2012	2013	2014
Osobno računalo	341,273	303,100	281,568
Tablet	120,203	184,431	263,229
Mobilni telefon	1,746,177	1,810,304	1,905,030

Izvor: [11]

Broj mobilnih terminalni uređaja je nadmašio ukupnu svjetsku populaciju 2014. godine, [12].

Tablica 2.2. Broj mobilnih terminalnih uređaja

[9] DVB-T - Digital Video Broadcasting - Terrestrial
[10] LTE-Long Term Evolution

Broj priključaka (u milijardama)	2014.	2020.	Postotak rasta
Pametni mobilni uređaji	2,7	6,1	225%
Mobilni širokopojasni uređaji	2,9	8,4	289%
Mobilni PC, tableti i ruteri	0,3	0,65	217%
Ukupno – mobilni terminalni uređaji	7,1	9,5	134%

Izvor: [13]

U Tablici 2.2. može se vidjeti previđanje porasta broja pametnih mobilni uređaja, mobilnih širokopojasnih uređaja te mobilnih PC-a, tableta i rutera u razdoblju od 2014. godine do 2020. godine, broj priključaka u tablici izražen je u milijardama.

3. Arhitektura Android i iOS operativnih sustava

U ovom poglavlju će biti opisana arhitektura Android i iOS operativnih sustava, sustava koji se nalaze na mobilnim terminalnim uređajima na kojima će se instalirati antivirusni alati. Kasnije će se napraviti komparativna analiza tih antivirusnih alata.

Mobilni operacijski sustavi upravljaju radom mobilnih uređaja te pružaju sučelje prema korisniku. Po načelima rada slični su operacijskim sustavima za stolna i prijenosna računala, no nešto su jednostavniji i više usmjereni bežičnom umrežavanju, mobilnim multimedijskim formatima (npr. 3GPP[11] File Format, QuickTime File Format, Advanced Audio Coding) i specifičnim metodama unosa podataka. Takve operacijske sustave obično koriste pametni telefoni, *PDA* (engl. *personal digital assistant*) uređaji, *tablet* računala i neki ugradbeni uređaji, [14].

3.1. Android operativni sustav

Tvrtka Android Inc. osnovana 2003. godine osnovna djelatnost bila je razvoj programske potpore za pametne mobilne uređaje. Dvije godine potom Google je kupio Android da bi 2007. godine inicirao osnivanje konzorcija OHA (*Open Handset Alliance*) s ciljem stvaranja javnog standarda za mobilne uređaje. Udruzi su odmah pristupile 34 firme različitih djelatnosti glede mobilne industrije poput proizvođača mobilnih telefona, programera aplikacija, mobilnih operatera i sličnih, da bi ubrzo imala preko 80 članova, [10].

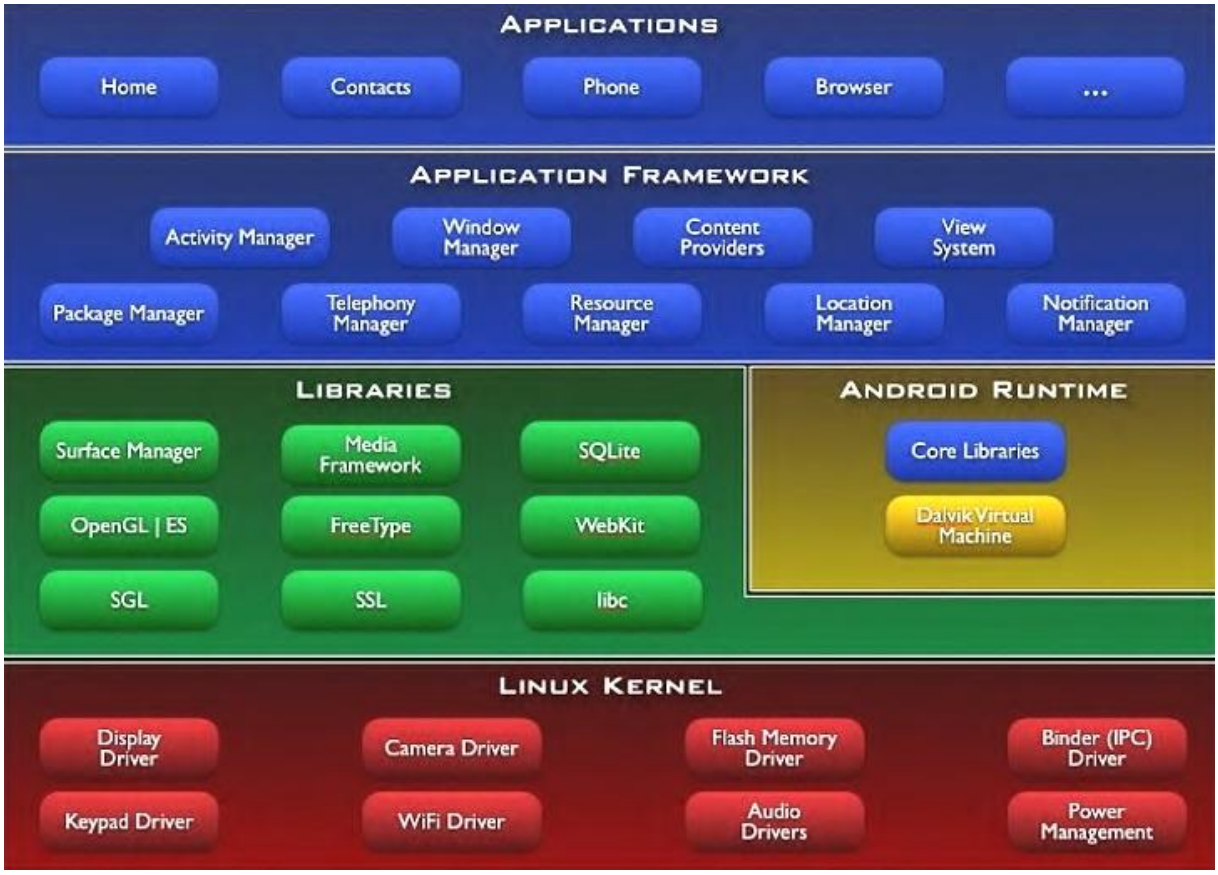
Sustav Android je mobilni operacijski sustav temeljen na Linux jezgri, a namijenjen je primarno izvođenju na procesorima koji sadrže ARM (engl. Advanced RISC Machines) jezgru opće namjene te ga odlikuju kvalitetno upravljanje potrošnjom energije uređaja, podrška za dodatno sklopovlje jednostavan razvoj aplikacija u programskom jeziku Java, [14].

Operativni sustav baziran je na programskom jeziku Java, ima ograničene resurse u pogledu procesne moći i memorijskih kapaciteta u odnosu na osobna računala jer su jezgra i arhitektura sustava prilagođeni za pokretanje i rad u ograničenim uvjetima kakvo je mobilno okruženje.

Osnovni dijelovi ovog okruženja su programske aplikacije koje koriste aplikacijske biblioteke (Framework), a na osnovama sistemskih biblioteka i sistemskih programskih rutina koje rabe Linux jezgru, kako prikazuje naredna slika, [10].

[11] 3GPP-3rd Generation Partnership Project – međunarodno regulatorno tijelo

Jezgra operativnog sustava brine o upravljanju memorijom, procesima, mrežnim sučeljima i ostalim sustavima na sklopovskom nivou, obrađuje osnovne usluge sustava i djeluje kao HAL (*Hardware Abstraction Layer*), među sloj između fizičkog sklopovlja i Android operativnog sustava. Tvorcima programske potpore jezgra nije dostupna. Sistemske biblioteke napisane su u C i C++ programskim jezicima zbog brzine izvođenja te su prilagođene svakom pojedinačnom uređaju.



Slika 3.1. Arhitektura Android operativnog sustava, [10]

Posebna osobitost je 'Dalvik virtualni sustav' (prema imenu razvojnog inženjera i firmi Google) koji dozvoljava izvršavanje više virtualnih strojeva odjednom kako bi se maksimalno iskoristio potencijal Linux jezgre. Odnosno, svaka aplikacija izvršava se u svom virtualnom okruženju. Sustav aplikacijskih biblioteka podloga je za razvoj korisničkih aplikacija. Aplikacije koje koriste operativni sustavu Android pripadaju najvišem sloju u prikazanoj arhitekturi. Za razliku od klasičnih aplikacija na stolnim računalima koje se paralelno izvode i imaju jednak prioritet, na ovoj platformi izvršava se jedna primarna aplikacija koja zauzima cijeli ekran, [10].

Sve instalirane aplikacije nalaze se na Android aplikacijskom sloju. Širok raspon aplikacija se može napisati pomoću aplikacijskog programskog sučelja razvojnih programera

ili korištenjem komponenata koje se mogu iskoristiti više puta od drugih aplikacija. Izvorno je Android već uključio nekoliko aplikacija sa osnovnim funkcionalnostima kao što su telefonski pozivi i upravljanje kontaktima. Međutim više prostora za popuniti je ostalo za programere. Programeri su ohrabreni da u potpunosti iskoriste značajke Androida pri pisanju vlastitih aplikacija, [15].

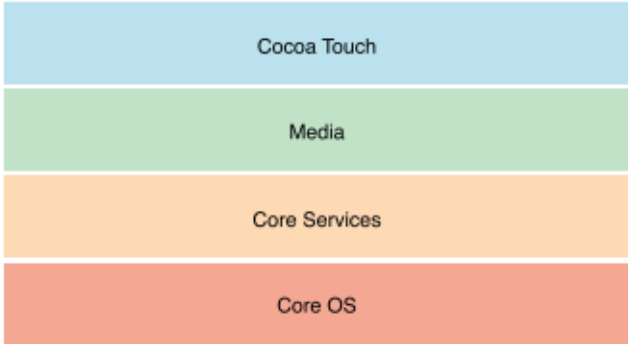
3.2. iOS operativni sustav

iOS je operativni sustav koji se pokreće na iPad, iPhone i iPod uređajima. Operativni sustav upravlja hardverom uređaja i pruža tehnologije potrebne za implementaciju izvornih aplikacija. Operativni sustav se također isporučuje sa različitim sistemskim aplikacijama kao što su telefoniranje, mail i safari preglednik koje pružaju standardne usluge sustava korisnicima, [16] .

Prva inačica operacijskog sustava iOS izdana je u lipnju 2007. godine - zajedno s uređajem iPhone (prve generacije). Sustav iOS nije imao službeno ime sve do ožujka 2008. godine kada je izdan iPhone SDK. Tada je dobio ime iPhone OS, da bi u lipnju 2011. godine bio preimenovan u iOS, [17].

Na najvišoj razini, iOS djeluje kao posrednik između temeljnog hardvera i aplikacije koja je kreirana. Aplikacije ne komuniciraju izravno sa temeljnih hardverom. Umjesto toga aplikacije komuniciraju sa hardverom putem skupa dobro definiranih sučelja sustava. Ta sučelja olakšavaju pisanje aplikacija koje rade na uređajima sa različitim hardverskim mogućnostima..

Implementacija iOS tehnologija može se promatrati kao skup slojeva koji su prikazani na slici. Niži slojevi sadrže osnovne usluge i tehnologije. Slojevi više razine nadograđuju slojeve niže razine pružaju sofisticirane usluge i tehnologije.



Slika 3.2. Implementacija iOS tehnologije, [16]

Jezgra operacijskog sustava iOS (engl. *kernel*) temeljena je na inačici Mach jezgre2 koja se koristi i u sustavu Mac OS X-u. Na toj su jezgri izgrađeni dodatni slojevi (engl. *layer*) za

implementaciju aplikacija na platformi. Na nižim slojevima su implementirane osnovne funkcionalnosti i tehnologije, a na višima one sofisticiranije i specijalizirane.

Core OS: Sadrži funkcionalnosti niže razine oko kojih je izgrađena većina ostalih tehnologija. Te funkcionalnosti programeri najčešće ne koriste izravno već kroz programska okruženja (engl. Framework). Iznimka su slučajevi kad je potrebna izravna komunikacija s vanjskim sklopovljem ili kad postoje sigurnosne prijetnje.

Core Services: Sadrži osnovne sistemske servise koje sve aplikacije koriste.

Media: Sadrži tehnologije za upravljanje grafikom, audio i video datotekama u cilju stvaranja multimedijski bogatih aplikacija.

Cocoa Touch: Sadrži ključna programska okruženja za izgradnju aplikacija za sustav iOS. Ovaj sloj definira osnovnu infrastrukturu aplikacije i daje podršku za tehnologije poput višezadaćnosti (engl. *multitasking*), unos putem ekrana osjetljivog na dodir, *push* obavijesti itd.

4. Sigurnosne prijetnje mobilnih terminalnih uređaja

Poput virusa i špijunskog softvera (*spyware*) koji mogu zaraziti vaše računalo, postoji niz sigurnosnih prijetnji koje mogu utjecati na mobilne uređaje. Prijetnje mobilnih uređaja možemo podijeliti u nekoliko kategorija: aplikacijski-bazirane prijetnje, web-bazirane prijetnje, mrežno-bazirane prijetnje i fizičke prijetnje.

4.1. Aplikacijski-bazirane prijetnje

Preuzete aplikacije mogu predstavljati mnoge vrste sigurnosnih problema za mobilne uređaje. Zlonamjerne aplikacije mogu izgledati dobro na stranicama sa kojih se preuzimaju, ali one su posebno napravljene kako bi se nanijela šteta korisniku. Čak se i legitiman softver može iskoristiti za prevare. Aplikacijsko bazirane prijetnje možemo uvrstiti u jednu ili više sljedećih kategorija:

a) **Malware** (zlonamjerni softver) je softver koji obavlja zlonamjerne radnje, a instaliran je na mobilnom uređaju. Bez znanja korisnika može napraviti troškove telefonskog računa slanjem neželjenih poruka korisnikovoj kontakt listi ili može napadaču omogućiti kontrolu nad korisnikovim uređajem.

b) **Spyware** (špijunski softver) je dizajniran za prikupljanje i korištenje osobnih podataka bez znanja ili odobrenja korisnika. Podaci koji su najčešće na meti *spyware*-a su povijest telefonskih poziva, SMS poruke, lokacija korisnika, povijest preglednika, popis kontakata, e-mail i privatne fotografije. Nabrojane informacije se mogu koristiti za krađu identiteta ili financijske prijevare.

c) **Prijetnje narušavanja privatnosti** mogu biti uzrokovane aplikacijama koje nisu nužno zlonamjerne, ali prikupljaju količinu podataka ili koriste osjetljive podatke (npr. lokacija, popis kontakata, osobni podaci) više nego je potrebno za obavljanje njihovih funkcija.

d) **Ranjive aplikacije** su aplikacije koje sadrže propuste koji se mogu iskoristiti za zlonamjerne svrhe. Takva ranjivost omogućuje napadaču pristup osjetljivim informacijama, obavljanje neželjenih radnji, sprječava pravilno funkcioniranje usluge ili preuzima aplikacije na mobilni uređaje bez znanja korisnika.

4.2. Web-bazirane prijetnje

Budući da su mobilni uređaji stalno spojeni na Internet i često se koriste za pristup web baziranim uslugama, web bazirane prijetnje predstavljaju potencijalne prijetnje za mobilne uređaje, a možemo ih podijeliti na, [18]:

a) **Phishing** (krađa identiteta) koristi e-mail, tekstualne poruke, društvene mreže za slanje linkova do web-stranica koje su dizajnirane da na prevaru od posjetitelja stranice saznaju informacije kao što su lozinke ili brojevi računa. Često su te poruke i web-stranice različite i mogu se razlikovati od stranica banaka korisnika ili drugih legitimnih izvora.

b) **Drive-BY** preuzimanja mogu automatski preuzeti aplikaciju kada se posjeti određena web-stranica. U nekim slučajevima korisnik mora poduzeti mjere kako bi pokrenuo preuzetu aplikaciju, a u nekim slučajevima se aplikacija pokreće sama automatski.

c) **Iskorištavanje preglednika**, iskorištava se ranjivost web preglednika ili softvera pokrenutog preko preglednika kao što je Flash player, PDF čitač ili preglednik slika. Jednostavnom posjetom nesigurne web-stranice, korisnik može aktivirati dodatak koji instalira zlonamjerni softver ili obavlja druge radnje na uređaju.

4.3. Mrežno bazirane prijetnje

Mobilni uređaji obično podržavaju mobilne mreže kao i lokalne bežične mreže (Wi-Fi, Bluetooth).Obje vrste mreža mogu biti napadnute od različitih klasa prijetnji, [18]:

a) **Iskorištavanje mreže**, iskorištavaju se nedostatci u mobilnim operativnim sustavima ili drugom softveru koji djeluje na lokalnoj ili mobilnoj mreži. Jednom povezani, mogu instalirati zlonamjerni softver na mobilni uređaj bez znanja korisnika.

b) **Wi-Fi Sniffing**, prikupljaju podatke koji putuju zrakom između uređaja i Wi-Fi pristupne točke. Mnoge aplikacije i web stranice ne koriste odgovarajuće sigurnosne mjere, slanje nekodiranih podataka preko mreže preko koje se lako može pročitati sadržaj koji treća strana može "uloviti" dok putuje mrežom.

4.4. Fizičke prijetnje

Mobilni uređaji su praktični za nošenje, vrijedni i nosimo ih gdje god pođemo, tako da njihova fizička sigurnost također može biti dovedena u pitanje te je važno razmotriti potencijalne prijetnje.

Izgubljen ili ukraden mobilni uređaj su jedne od najčešćih prijetnji mobilnim uređajima. Mobilni uređaj je vrijedan ne samo zbog vrijednosti hardvera koji se može prodati na crnom tržištu već i zbog osjetljivih osobnih podataka i poslovnih podataka koji se mogu na njemu nalaziti, [18].

5. Antivirusni alati

Mobilni antivirusni alati su programi za otkrivanje i zaštitu, prepoznavanje i uklanjanje virusa na mobilnim uređajima. Moderna antivirusna rješenja mogu štitit mobilne uređaje od širokog spektra zlonamjernih programa uključujući crve, viruse i trojanske konje.

5.1. Lookout

Lookout su 2007. godine osnovali John Hering, James Burgess i Kevin Mahaffey s pretpostavkom da je za zaštitu ljudi i poduzeća od mobilnih napada potreban novi pristup sigurnosti-onaj koji ukorijenjen u analizi podataka, radi na nevjerojatnim razmjerima i oslanja se na predvidljivoj strojnoj inteligenciji, [18].

Lookout dolazi u dvije verzije, besplatnoj i Premium. Istraživanje će se obaviti sa besplatnom verzijom Lookout aplikacije, aplikacija za Android uređaj je preuzeta sa Androidovog servisa za preuzimanje aplikacija Google Play-a, a za iOS uređaj sa Apple-ovog servisa App store-a. U Tablici 5.1 su prikazane funkcionalnosti koje dolaze u besplatnoj, a koje u Premium verziji.

Tablica 5.1. Usporedba funkcionalnosti besplatne i Premium verzije Lookout aplikacije

	Besplatna verzija	Premium verzija
Sigurnost i privatnost		
Prediktivna sigurnost	✓	✓
Savjetnik za privatnost		✓
Sigurno pretraživanje		✓
Zaštita od krađe		
Lociranje	✓	✓
Zvučno upozorenje	✓	✓
Odbljesak signala	✓	✓
Upozorenje o krađi		✓
Zaključavanje uređaja		✓
Sigurnosno kopiranje podataka		
Sigurnosno kopiranje kontakata	✓	✓
Sigurnosno kopiranje slika		✓
Sigurnosno kopiranje povijesti poziva		✓

Preuzimanja i prijenos podataka	✓	✓

Izvor: [18]

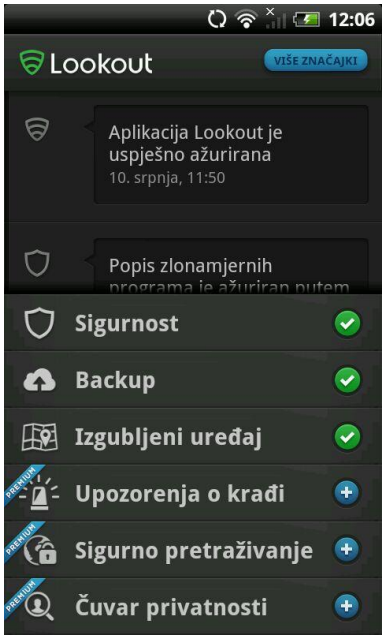
5.1.1. Podešavanje Lookout aplikacije

Lookout aplikacija preuzeta je sa Google Play trgovine, veličine je 8.54 MB, preuzeta verzija je besplatna te ima više od 100 milijuna preuzimanja.

Nakon instaliranja aplikacije bilo je potrebno napraviti Lookout račun, prednost pri instaliranju je ta što nije potrebno izlaziti iz aplikacije što dodatno ubrzava njeno instaliranje.

Kretanje po Lookout-ovom sučelju je jako intuitivno. Gornja polovica ekrana u aplikaciji se može pomicati dolje-gore i u njoj možemo vidjeti nedavne aktivnosti kao što su rezultati skeniranja ili ažuriranja. Donja polovica ekrana aplikacije čini šest tipaka: Sigurnost, Backup, Izgubljeni uređaj, upozorenje o krađi, Sigurno pretraživanje, Čuvar privatnosti koje su prikazane na slici 20.

Zelena kvačica kraj tipke označava je li funkcionalnost omogućena, ukoliko se nalazi bijeli plus na plavoj pozadini znači da funkcionalnost nije omogućena.



Slika 5.1. Sučelje Lookout aplikacije

Ukoliko se klikne na jednu od ovih 6 funkcionalnosti otvorit će se podizbornik s dodatnim alatima i specifičnim informacijama.

Na primjer izbornik Backup nudi izradu Backup-a kontakata, fotografija ili povijesti poziva. Besplatna verzija koja je korištena u istraživanju nudi samo backup kontakata što se vidi na slici 5.2.

Na početnom zaslonu aplikacije kod mobilnih terminalnih uređaja sa većim ekranom nalazi se tipka sa tri točke tj. dodatan izbornik sa postavkama , računom, pomoći, mogućnosti podjele te informacije o Lookout-u.

Slika 5.2. Podizbornik izbornika Backup

Na testiranom mobilnom terminalnom uređaju HTC Desire HD potrebno je pritisnuti *Menu* tipku uređaja da bi se otvorio taj izbornik.

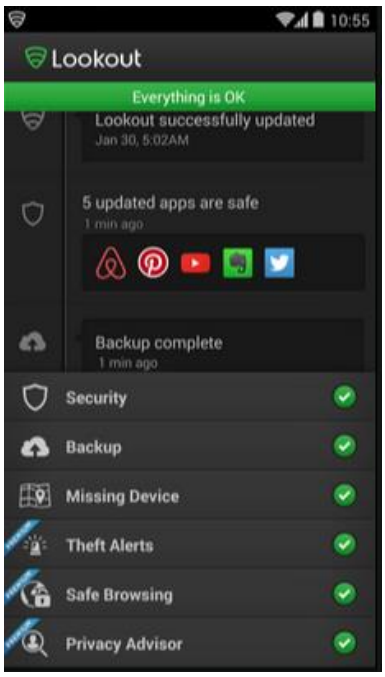
5.1.2. Funkcionalnosti Lookout aplikacije

U ovom pod poglavlju će biti objašnjene funkcionalnosti koje nudi Lookout aplikacija te koje su navedene u Tablici 5.1.

iOS-ova verzija antivirusnog alata ne sadrži funkcionalnost sigurnog pretraživanja u niti jednoj verziji dok je razlika između besplatne verzije i Premium verzije ta što u Premium verziji postoji funkcionalnost obavijesti o krađi i sigurnosno kopiranje slika.

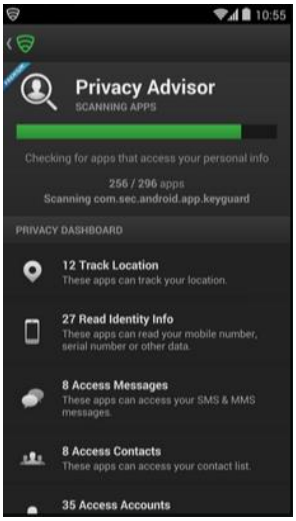
Prvu kategoriju čine funkcionalnosti vezane za sigurnost i privatnost. U besplatnoj verziji se može koristiti prediktivna sigurnost (*Predictive Security*) dok Premium verzija nudi još i savjetnik za privatnost (*Privacy Advisor*) te sigurno pretraživanje (*Safe Browsing*).

Prediktivna sigurnost omogućuje pouzdanije praćenje postojećih prijetnji i preciznije predviđanje "*zero day*" prijetnji.



Slika 5.3. Prediktivna sigurnost, [18]

Savjetnik za sigurnost omogućuje prikaz informacija kojima može pristupiti određena aplikacija npr. lokacija ili korisnikovi kontakti te korisnik čime korisnik može bolje zaštiti svoje privatne podatke.



Slika 5.4. Savjetnik za privatnost, [18]

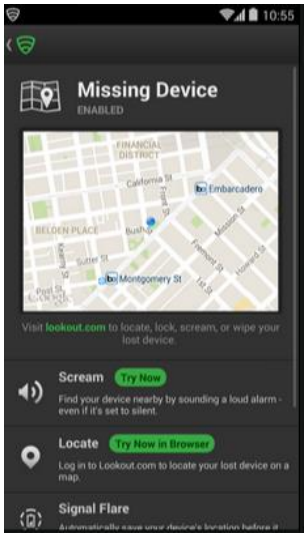
Prilikom pronalaska potencijalnih prijetnji, rezultat pretraživanja se prikazuje na početnom zaslonu aplikacije s mogućnošću otvaranja dodatnog izbornika.

Sigurno pretraživanje štiti korisnika pri pretraživanju internet stranica od sumnjivih web stranica koje bi mogle zaraziti korisnikov uređaj ili otuđiti korisnikove osobne podatke.

Slika 5.5. Sigurno pretraživanje, [18]

U drugu kategoriju pripadaju funkcionalnosti zaštite od krađe. U besplatnoj verziji se može koristiti lociranje (*Locate*), odbljesak signala (*Signal Flare*) i zvučno upozorenje (*Scream*) dok Premium verzija nudi još i upozorenje o krađi (*Theft Alerts*) i zaključavanje uređaja (*Lock* & *Wipe*).

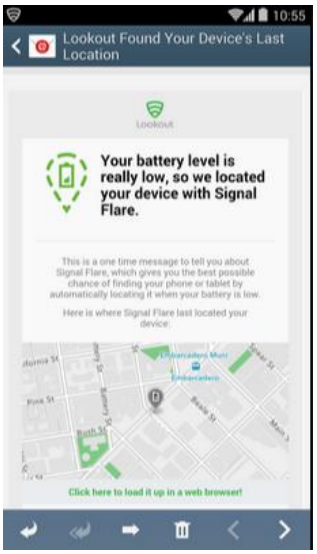
Lociranje i **zvučno upozorenje** omogućuju određivanje pozicije mobilnog terminalnog uređaja na karti kada je izgubljen te aktiviranje glasnog zvučnog upozorenja (alarm) čak iako su na uređaju isključeni zvukovi.



Slika 5.6. Lociranje i zvučno upozorenje, [18]

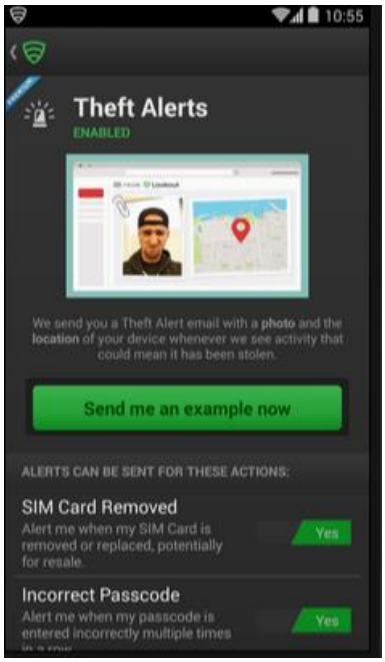
Odbljesak signala će automatski spremiti posljednju lokaciju uređaja prije nego se baterija uređaja isprazni kako bi kad se znala lokacija kad se potpuno ugasi uređaj.

Odbljesak signala dolazi u obje verzije Lookout antivirusnog alata te također i na oba operativna sustava koja su korištena u istraživanju.



Slika 5.7. Odbljesak signala, [18]

Upozorenje o krađi će poslati fotografiju i lokaciju uređaja na email korisnika ukoliko se prijeti da je uređaj ukraden.



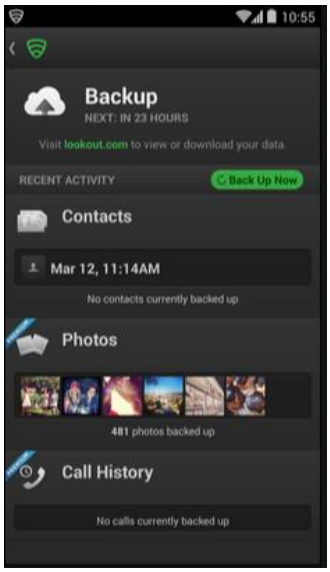
Slika 5.8. Upozorenje o krađi, [18]

Prijavom na stranici Lookout.com sa bilo kojeg internet pretraživača moguće je zaključati uređaj te obrisati osobne podatke ukoliko je uređaj ukraden, putem funkcionalnosti **zaključavanja uređaja**.

Na slici 5.9 prikazano je web sučelje putem kojeg korisnik može locirati svoj uređaj, uključiti alarm, zaključati ga ili pobrisati tekstualne poruke, fotografije, kontakte, prijave i ostale podatke s izgubljenog mobilnog terminalnog uređaja.

Slika 5.9. Zaključavanje uređaja, [18]

Posljednja kategorija je sigurnosno kopiranje podataka. Besplatna verzija omogućava **kopiranje kontakta** (*Contacts*) i **prijenos podataka** (Data Transfer) dok Premium verzija nudi još i **sigurnosno kopiranje slika** (*Photos*) te povijest poziva (*Call History Backup*).



Slika 5.10. Sigurnosno kopiranje podataka, [18]

Verzija aplikacije na iOS operativnom sustavu ima iste mogućnosti izrade sigurnosnog kopiranja podataka kao i Android verzija.

5.1.3. Otkrivanje sigurnosnih prijetnji i performanse

Pokretanjem opcije „*Scan now*“ u izborniku Security pokreće se skeniranje instaliranih aplikacija na mobilnom terminalnom uređaju. Prilikom skeniranja u dijalogu za skeniranje se prikazuje ikona aplikacije koja se skenira. Moguće je napraviti i raspored za skeniranje na dnevnoj ili tjednoj bazi kao i određeni dan u određeno vrijeme koje korisnik sam odredi.

Za zaštitu u realnom vremenu, Lookout automatski skenira preuzete aplikacije i file-ove te blokira pristup web stranicama koje sadrže *malwere* ili su poznate kao *phishing* web stranice. Značajka sigurnosnog pregledavanja radi sa pred instaliranim android preglednikom i Chrome Android preglednikom za Android.

5.2. Avast Mobile Security

AVAST Software osnovali su Pavel Baudiš i Eduard Kučera 1991. godine u Češkoj, a sada ima urede širom svijeta. Proizvode *freeware* i *shareware* sigurnosne proizvode pod brandom Avast za osobne i komercijalne potrebe za PC, MAC i Android uređaje s korisničkim sučeljem dostupnim na 45 jezika. Od 2013. godine više od 200 milijuna uređaja širom svijeta koristi Avast, a od siječnja 2014. godine ima gotovo 16 % tržišnog udjela na tržištu koje se bavi sigurnošću. Avast trenutno štiti više od 25 milijuna Android uređaja, [19].

Aplikacije dolazi u dvije verzije, besplatnoj i Premium. Istraživanje će se obaviti sa besplatnom verzijom Lookout aplikacije, aplikacija za Android uređaj je preuzeta sa Androidovog servisa za preuzimanje aplikacija Google Play-a.

5.2.1. Podešavanje Avast aplikacije

Avast aplikacija preuzeta je s Google Play trgovine, veličine je 10.52 MB, preuzeta verzija je besplatna te ima više od 100 milijuna preuzimanja.

Kod instaliranja može se napraviti Avast račun ali sve funkcionalnosti koje se nalaze u besplatnoj verziji aplikacije rade i bez izrade računa. Funkcionalnosti izrade sigurnosne kopije i zaštite protiv krađe nisu integrirane u ovoj aplikaciji nego se moraju posebno preuzeti što je nedostatak .

Kretanje po Avast-ovom sučelju je jako intuitivno. Indikator stanja na vrhu početnog zaslona omogućuje da korisnik vidi na prvi pogled koje su značajke omogućene (zeleno), ako su neke onemogućene (narančasto) i ako su sve onemogućene (crveno). Ispod indikatora statusa

su funkcionalnosti skeniranje virusa, Wi-Fi sigurnost, sigurnost protiv krađe i zaključavanje aplikacija te više alata.

Pritiskom na više alata otvara se skočni prozor s dodatnim funkcionalnostima kao što su savjetnik za sigurnost, upravljanje aplikacijama, filter za pozive i sms-ove, vatrozid i mjerač prometa. Pri dnu ekrana nalazi se zapis nedavnih aktivnosti. Pritiskom na gumb otvara se novi prozor s dodatnim pojedinostima o tome koje su aplikacije skenirane te koje su zaštitne značajke omogućene ili onemogućene.

Pritiskom tipke *menu* na kada se nalazimo glavnom izborniku, otvara se izbornik sa postavkama, ocjenom aplikacije, linkom za ostale Avast aplikacije te računu na koji je korisnik prijavljen. U izborniku postavke korisnik može promijeniti svoj Avast PIN, promjena jezika, upravljati automatskim ažuriranjem i omogućiti dodatne mogućnosti kao što je PUP detekcija, CPU Wakelock.

5.2.2. Funkcionalnosti Avast aplikacije

U ovom pod poglavlju biti će objašnjene funkcionalnosti koje nudi Avast aplikacija. Većina opisanih funkcionalnosti nalazi se u besplatnoj verziji aplikacije koja će biti korištena u istraživanju.

Skeniranje virusa kao što i sama riječ govori koristi se za skeniranje virusa na mobilnim terminalnom uređaju. Postoji mogućnost skeniranja aplikacija ili ostalih file-ova

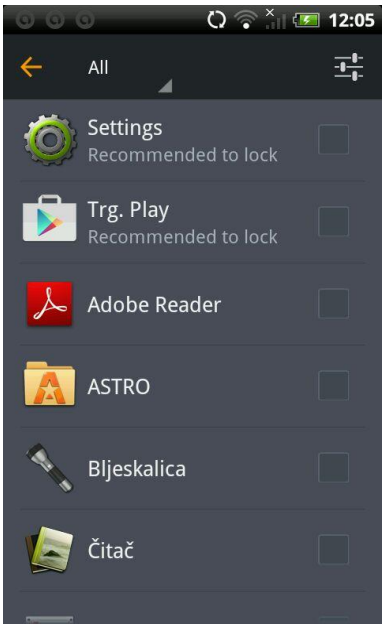
Slika 5.11. Skeniranje virusa

. Aplikacija nudi trenutno skeniranje ili postavljanje automatskog skeniranja koje korisnik može podesiti ovisno o svojim potrebama.

Wi-Fi sigurnost se koristi za provjeru sigurnosti Wi-Fi –a na koji je spojen mobilni terminalni uređaj.

Slika 5.12. Wi-Fi sigurnost

Zaključavanje aplikacija se koristi kako bi se zaključale određene aplikacije. Kod pokretanja aplikacija korisnik će morati upisati pin kako bi joj mogao pristupiti. Za ovu funkcionalnost potrebna je prijava na Avast račun ili dodavanje sekundarnog mobilnog broja na koji će biti poslan pin.



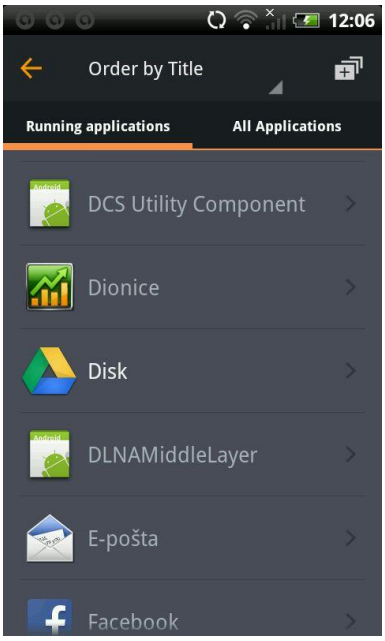
Slika 5.13. Zaključavanje aplikacija

Savjetnik za sigurnost omogućuje prikaz informacija kojima može pristupiti određena aplikacija npr. lokacija ili korisnikovi kontakti te korisnik čime korisnik može bolje zaštiti svoje privatne podatke. Ovdje još postoji **Ad Detector** opcija koja nudi još detaljniji prikaz ukoliko

neka aplikacija izvršava sama radnje kao što je prikupljanje informacija o lokaciji, prikupljanje informacija o mreži, postavljanje ikona na početni ekran korisnika, prikaz oglasa u traci za obavijesti.

Slika 5.14. Savjetnik za sigurnost

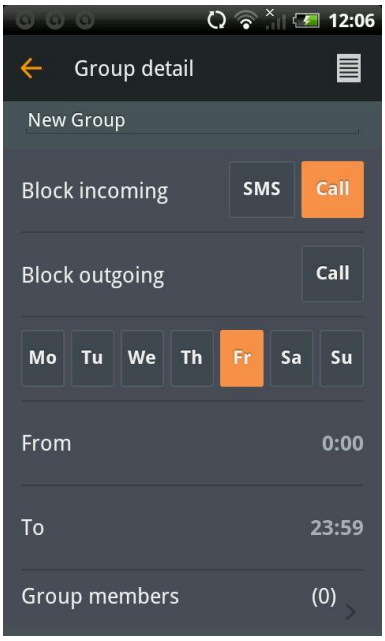
Upravljanje aplikacijama nudi prikaz svih aplikacija instaliranih na mobilnom terminalnom uređaju i aplikacija koje su trenutno pokrenute, također nudi prikaz informacija o aplikaciji kao što su veličina aplikacije, zauzimanje memorije, posljednje korištenje itd.



Slika 5.15. Upravljanje aplikacijama

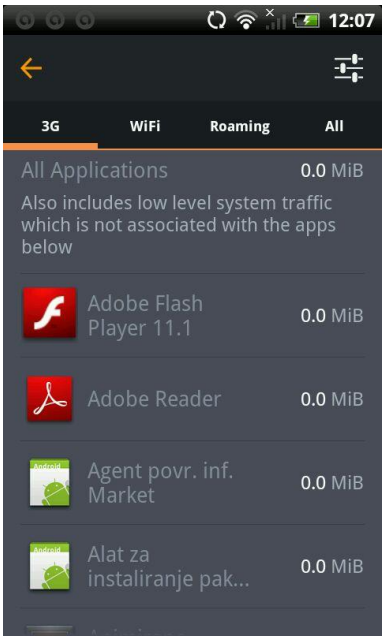
Upravljanje aplikacijama nudi i mogućnost brisanja aplikacija koje se nalaze na mobilnom terminalnom uređaju korisnika

Filter poziva i SMS poruka koristi se kako bi se blokirali dolazni SMS-ovi ili pozivi u određeno vrijeme i od određenih kontakata, također se može blokirati i odlazni poziv.



Slika 5.16. Filter poziva i SMS-ova

Mjerač prometa prikazuje potrošnju internet prometa, podijeljena je potrošnja na 3G, Wi-Fi, *Roaming* te ukupna potrošnja kao što je prikazano na slici 5.17.



Slika 5.17. Mjerač prometa

Prilikom korištenja mjerača prometa korisnik može odrediti dane u mjesecu kada želi da se mjesečne ili godišnje statistike vrate na početnu vrijednost odnosno da se resetiraju.

5.2.3. Otkrivanje sigurnosnih prijetnji i performanse

Pritiskom na tipku *Run Scan* u izborniku Virus Scanner pokreće se ručno skeniranje koje skenira instalirane aplikacije. Također može se podesiti da se skeniraju sve preuzete ili označene datoteke. Ukoliko korisnik ne želi sam svaki puta pokretati skeniranje, može namjestiti automatsko skeniranje u određene dane u tjednu i vremenu po izboru.

U smislu zaštite u realnom vremenu, Avast automatski skenira aplikacije koje su instalirane i pokrenute, također skeniraju se i file-ovi kada se čitaju ili se mijenjaju, pregledavaju se dolazne tekstualne poruke te se skeniraju URL-ovi zbog virusa u zlonamjernog ponašanja.

5.3. Trend Micro Mobile Security

Trend Micro osnovan je 1988 godine u Los Angeles-u. Danas je sjedište kompanije u Tokiju u Japanu. Steve Chang je tvrtku osnovao 1988. godine te je do danas stekla visoku reputaciju za svoje tehnološke inovacije. Počevši sa zaštitom od virusa za radne stanice, tvrtka se danas bavi i antivirusnom zaštitom mrežnih servera i ulaza/izlaza na internetu. Tvrtka Trend Micro se fokusira na prevenciju šteta koje mogu nanijeti mrežni crvi (*worms*) i virusi i savjetuje korisnike putem inicijativa kao što je Trend Micro Enterprise Protection Strategy.

Trend Micro je izgradio ugled pretvarajući dobre ideje u vrhunsku tehnologiju. Povodom priznanja za strategiju i viziju, najveći svjetski analitičari informatičkih tržišta, Gartner Group, je proglasio Trend Micro za vizionara na svom području djelovanja, 4 godine za redom. U samo jednom desetljeću, Trend Micro, sa sjedištem u Tokyu, izrastao je u multinacionalnu organizaciju s više od 2000 zaposlenika u više od 30 zemalja. Prihodi Trend Micro-a u 2003. godini nadmašili su prethodnu godinu dostigavši 454 milijuna američkih dolara, [20].

Trend Micro dolazi u dvije verzije, besplatnoj i Premium. Istraživanje će se obaviti sa besplatnom verzijom Lookout aplikacije, aplikacija za Android uređaj je preuzeta sa Androidovog servisa za preuzimanje aplikacija Google Play-a. Besplatna verzija aplikacije nudi mogućnost korištenja Premium funkcionalnosti 30 dana, a nakon toga se može nadograditi besplatna verzija na Premium ili nastaviti koristiti besplatnu verziju bez Premium funkcionalnosti.

U Tablici 5.2 su prikazane funkcionalnosti koje dolaze u besplatnoj, a koje u Premium verziji.

Tablica 5.2.Usporedba funkcionalnosti besplatne i Premium verzije Trend Micro aplikacije

	Besplatna verzija	Premium verzija
Zaštita od virusa		
Blokiranje Malware-a		✓
Skeniranje aplikacija	✓	✓
Neograničeno ažuriranje	✓	✓
Skeniranje „oblaka“	✓	✓
Čistač Malware-a		✓
Prevencija krađe podataka		
Skener privatnosti		✓
Sigurnost naplate	✓	✓
Sigurno surfanje		
Blokiranje zlonamjernih web stranica		✓
Roditeljska zaštita		✓
Blokiranje poziva i tekstualnih poruka		
Blokiranje poziva i tekstualnih poruka		✓
Zaštita izgubljenog uređaja		
Lociranje uređaja		✓
Zvučno upozorenje		✓
Udaljeno zaključavanje		✓
Udaljeno brisanje		✓
Zaštita SIM karticom		✓
Posljednja lokacija		✓
Spremanje lokacije kod pražnjenja baterije		✓
Online pohrana		
Sigurnosno spremanje i vraćanja	50 MB	50 MB
Sigurnosno spremanje i vraćanje kontakata između Androida i iOS-a	✓	✓
Privatnost društvenih mreža		
Skeniranje Facebook-a	✓	✓
Optimizacija sustava		
Upravitelj aplikacija		✓
Optimiziranje baterije	✓	✓
Pametna ušteda energije		✓
Jednostavan telefon	✓	✓
Automatski jednostavan telefon		✓
Optimiziranje memorije	✓	✓
Čišćenje povijesti	✓	✓
Podrška i više		
Online tehnička podrška	✓	✓
Zaštita deinstaliranja		✓
Bez reklama		✓

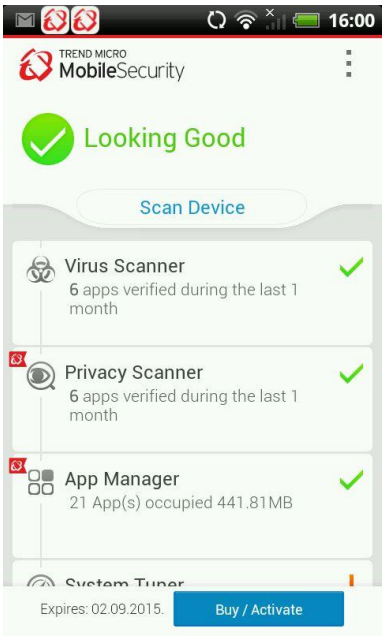
Izvor: [31]

5.3.1. Podešavanje Trend Micro aplikacije

Trend Micro aplikacija preuzeta je s Google Play trgovine, veličine je 11.10 MB, preuzeta verzija je besplatna te ima više od 50 tisuća preuzimanja.

Nakon instaliranja aplikacije bilo je potrebno napraviti Lookout račun, prednost pri instaliranju je ta što nije potrebno izlaziti iz aplikacije što dodatno ubrzava njeno instaliranje.

Sučelje aplikacije je intuitivno. Kada se pokrene aplikacija, na početnom zaslonu prvi vrhu ekrana nalaze se obavijesti o posljednjem skeniranju te tipka za početak skeniranja.



Slika 5.18. Sučelje Trend Micro aplikacije

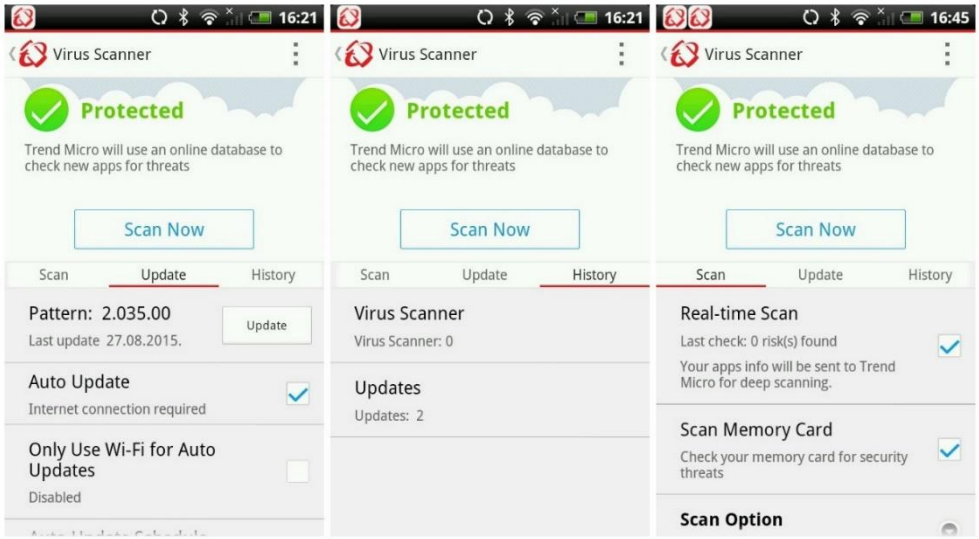
U desnom gornjem kutu se nalaze tri točkice koje označavaju izbornik koji nudi postavke, aktiviranje Premium verzije, pomoć, dijeljenje i ocjenu aplikacije. Ispod dijela za obavijesti poredane su funkcionalisti koje možemo detaljno pregledati klikom na njih klizanjem gore/dolje.

5.3.2. Funkcionalnosti Trend Micro aplikacije

U ovom pod poglavlju će biti objašnjene funkcionalnosti koje nudi Trend Micro aplikacija te koje su navedene u Tablici 5.2. Tvrtka Trend Micro je podijelila funkcionalnosti u kategorije od kojih se svaka kategorija odnosi na poseban dio zaštite.

Prva kategorija se odnosni na **zaštitu od virusa**. U ovu kategoriju se svrstava blokiranje *malwarea*, skeniranje aplikacija zbog mogućih virusa, ažuriranja baze virusima, skeniranje *cloud*-a.

Slika 5.19. prikazuje sve podizbornike skeniranja virusa i njihove opcije koje korisnik može uključivati prema vlastitoj želji ili potrebi.



Slika 5.19. Podizbornik skeniranja virusa

Skeniranje virusa omogućuje skeniranje svih instaliranih aplikacija i preuzetih kako bi se filtrirali mogući virusi i zlonamjerne aplikacije koje mogu neovlašteno preuzimati korisnikove informacije ili raditi novčane troškove.

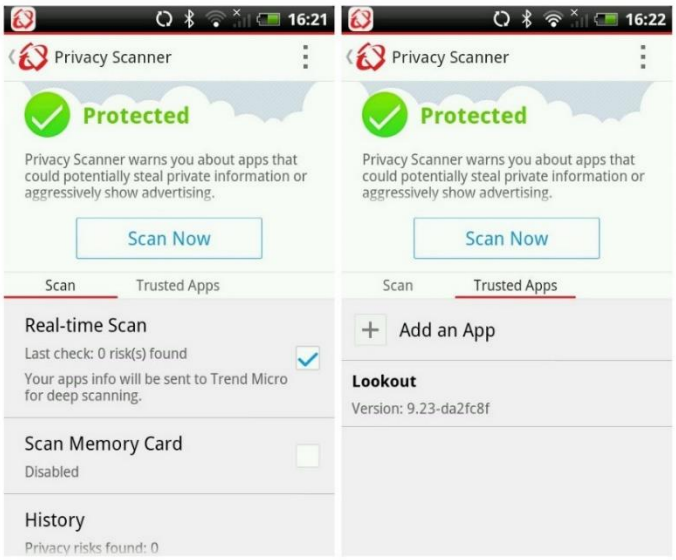
Druga kategorija se odnosi na **sigurnost korisničkih podataka**, skeniraju se sve aplikacije kako bi se otkrile one koje prikupljaju i kradu korisničke podatke. Ova funkcionalnost je odstupana samo u Premium verziji ili u probnom razdoblju. Također postoji i poseban sloj zaštite od lažnih aplikacija koje se odnose na financije, bankarstvo ili kupovinu jer također mogu ukrasti korisnikov novac ili identitet uvjeravajući korisnika da su legitimne aplikacije.

Na slici 5.20 mogu se vidjeti opcije podizbornika skenera privatnosti. Na lijevoj strani slike može se vidjeti stanje od prošlog skeniranja i uključiti opcija skeniranja u realnom vremenu, uključiti skeniranje i memorijske kartice te pregledati povijest skeniranja.

Na desnoj strani korisnik može sam napraviti popis aplikacija kojima vjeruje, klikom na te dodane aplikacije korisnik se preusmjerava na stranice Trend Micro-a gdje se nalaze informacije što radi pojedina aplikacija tj. koje su joj korisničke informacije dostupne.

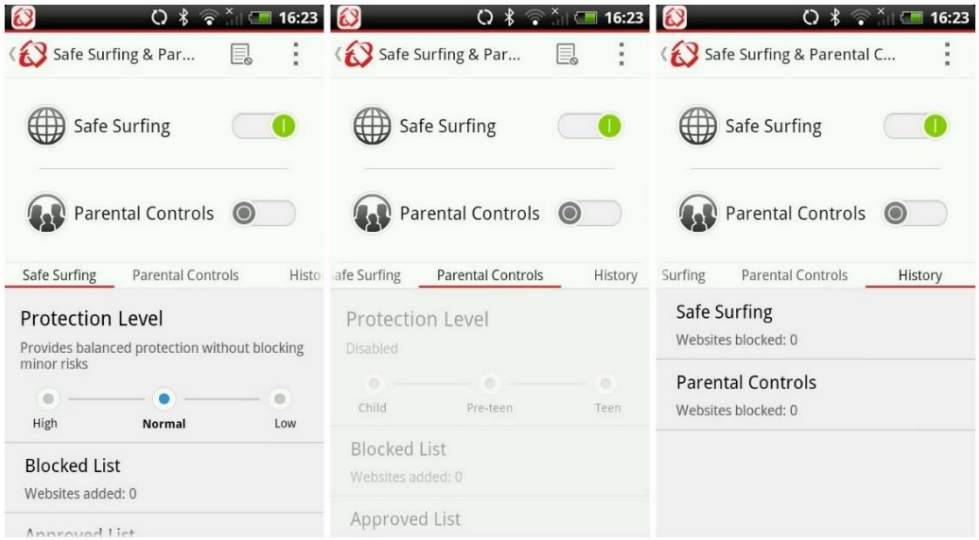
Klikom na opciju history korisnik može provjeriti prijašnje pronađene prijetnje ili novo otkrivene prijetnje, također nudi mu se opcija da sazna više detalja o označenoj prijetnji odnosno aplikaciji, nudi mu se mogućnost brisanja te aplikacije ili ukoliko je mišljenja da je aplikacija sigurna i da ne predstavlja potencijalnu prijetnju za njegov mobilni terminalni uređaj može je označiti kao sigurnu.

Prilikom pronalaska potencijalne prijetnje, korisnik dobiva obavijest, na testiranom uređaju HTC Desire HD obavijest se pojavljuje u traci za obavijesti na vrhu ekrana.



Slika 5.20. Podizbornik skenera privatnosti

Treća kategorija se odnosni na **sigurno surfanje**, omogućuje blokiranje zlonamjernih web stranica i nudi opciju roditeljske zaštite kako bi se određene stranice mogle filtrirati zbog sadržaja na njima.

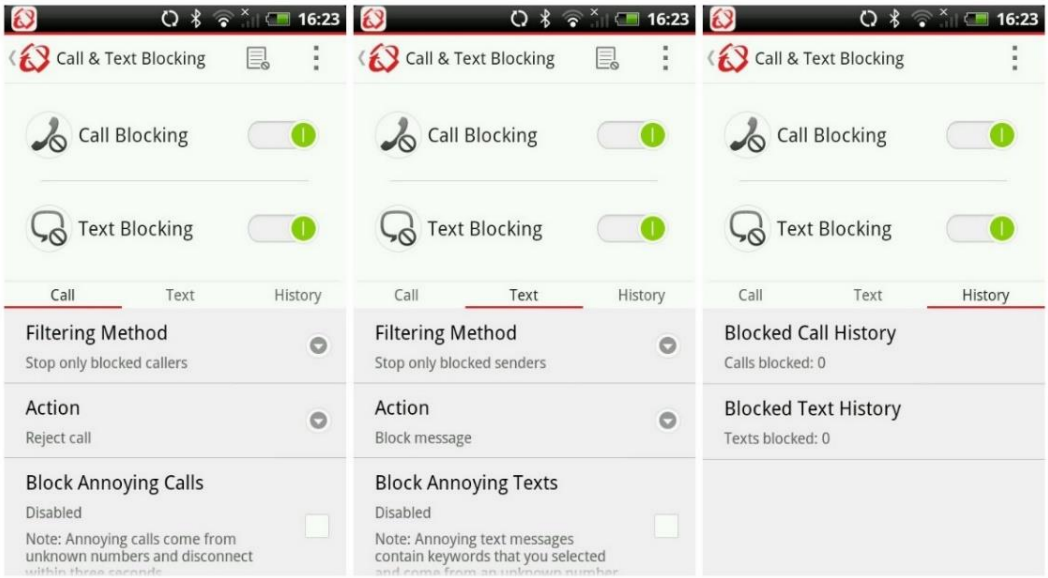


Slika 5.21. Podizbornik sigurnog surfanja i roditeljske zaštite

Korisnik može sam isključivati opciju sigurnog surfanja te odrediti koju razinu blokiranja web stranica želi, ponuđene su 3 razine (*High*,*Normal* i *Low*) također mogu se dodavati stranice koje da se blokiraju i koje da se ne blokiraju ukoliko određene postoje. Kod roditeljske zaštite postoje 3 razine (*Child*,*Pre-teen* i *Teen*), mogu se odrediti koje stranice će

biti blokirane, a koje su sigurne te još postoji zaštita od neovlaštenog brisanja. U History dijelu mogu se vidjeti sve blokirane stranice iz sigurnog surfanja i roditeljske zaštite.

Četvrta kategorija naziva se **blokiranje poziva i poruka** kao i sama funkcionalnost, filtriraju se neželjeni pozivi i poruke na temelju ključnih riječi, anonimnih poziva, bijele liste ili crne liste.

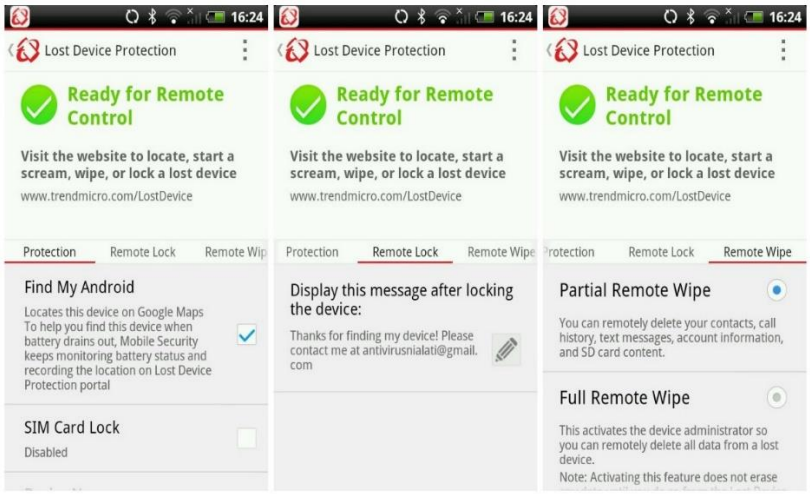


Slika 5.22. Podizbornik blokiranja poziva i poruka

Kada se uđe u podizbornik Call & Text Blocking nudi se mogućnost aktiviranja opcija blokiranja poruka i poziva. Metoda filtriranja kod poziva nudi tri opcije, onemogućeni pozivi samo blokiranim pozivateljima, dopuštanje samo odobrenim pozivateljima i dopuštanje pozivateljima koji su odobreni i anonimni. Kod radnji koje će se dogoditi kad se poziv odbija također su tri opcije, klasično odbijanje poziva, stišavanje uređaja i odbijanje i slanja poruke pozivatelju. Postoji mogućnost blokiranja nepoznatih brojeva koji se prekidaju nakon 3 sekunde. Kod blokiranja tekstualnih poruka nudi se opcija blokiranja brojeva na blok listi ili dopuštanja od onih brojeva koji su na listi dopuštenih pošiljatelja. Radnje su blokiranje poruka, blokiranja i brisanje poruke te blokiranje poruke te odgovor porukom. Također postoji mogućnost pregledavanja povijesti blokiranih poziva i poruka.

Peta kategorija odnosi se na **zaštitu izgubljenog uređaja**. Nudi se mogućnost lociranja izgubljenog uređaja, zaključavanje uređaja udaljenim putem te brisanje korisničkih podataka sa uređaja.

Ulaskom u podizbornik nudi se opcija lociranja uređaja preko Google Maps-a u slučaju kada je baterija na niskoj razini, aplikacija nadzire status baterije i snima posljednju lokaciju ukoliko dođe do gašenja uređaja.

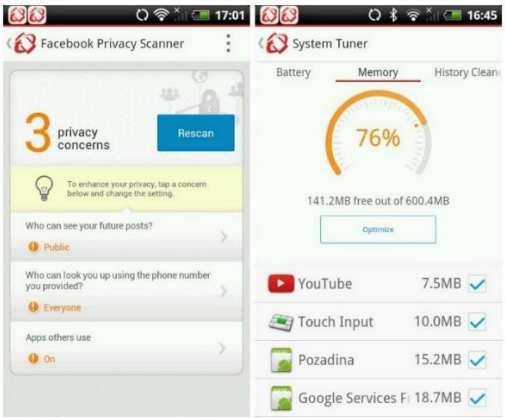


Slika 5.23. Podizbornik zaštite izgubljenog uređaja

Postoji opcija zaključavanja uređaja ukoliko se izvadi SIM kartica iz uređaja. Kod zaključavanja uređaja moguće je ostaviti poruku na zaslonu zaključanog uređaja. Kako bi se zaštitili korisnički podaci moguće je moguće je brisanje istih udaljenim putem što uključuje brisanje kontakata, povijesti poziva, poruka, informacija o računu ili sadržaja sa SD kartice.

U šestu kategoriju se svrstava **online pohrana**, omogućuje izradu sigurnosne kopije podataka u *cloud* i vraćanje podataka na uređaj za koji se korisnik odluči. Da bi se koristila ova funkcionalnost potrebna je dodatna instalacija aplikacije za rad sigurnosnih kopija i vraćanje podataka.

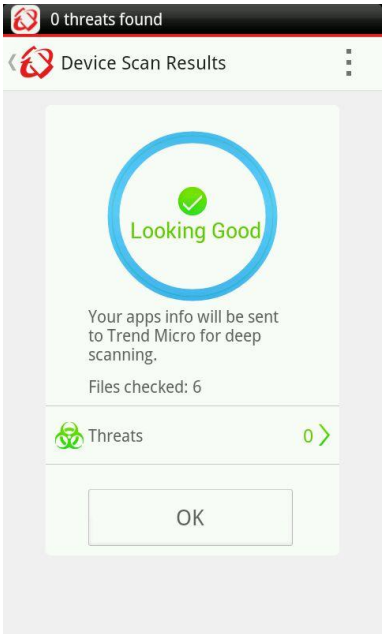
Trend Micro Mobile Security aplikacija nudi i **zaštitu korisničkih podataka na društvenoj mreži Facebook** te **optimiziranje uređaja** u segmentu baterije i memorije što je prikazana na slici 5.24.



Slika 5.24. Podizbornici skeniranja Facebooka-a i optimiziranje baterije i memorije uređaja

5.3.3. Otkrivanje sigurnosnih prijetnji i performanse

Pritiskom na tipku Scan Device koja se nalazi pri vrhu ekrana u početnom izborniku pokreće se ručno skeniranje koje skenira instalirane aplikacije i ostale podatke na uređaju.



Slika 5.25. Skeniranje u Trend Micro aplikaciji

Automatsko skeniranje je moguće nakon ažuriranja koje se može namjestiti na dnevnoj, tjednoj ili mjesečnoj bazi.

5.4. McAfee Mobile Security

Tvrtka Mcafee najveća je svjetska tvrtka za sigurnost, osnovana je 1987 godine, osnovao ju je John McAfee. Nude zaštitu računala klijenata od najnovijih prijetnji te uz pomoć svoje usluge Global Threat Intelligence prate nove prijetnje.

Nude i zaštitu za mobilne uređaje, uključujući i mogućnost pronalaska izgubljenih ili ukradenih uređaja i osnovnu zaštitu identiteta, da bi novac te osobne i bankovne informacije bile sigurne. Sjedište kompanije je u Santa Clari u Kaliforniji. Od 2011. godine tvrtka je u vlasništvu Intel-a.

Podržani operacijski sustavi za uređaj su Google Android 2.3 ili novija verzija, uključujući Android 5.x (Android L) te Google Android 4.4 ili novija verzija za sat Android Wear. U istraživanju će se koristiti besplatna verzija, Premium verzija se naplaćuje 29.99 eura godišnje.

5.4.1. Podešavanje Mcafee aplikacije

Mcafee aplikacija preuzeta je s Google Play trgovine, veličine je 12.81 MB, preuzeta verzija je besplatna te ima više od 10 milijuna preuzimanja.

Nakon instaliranja potrebno je prihvatiti uvjete korištenja, odmah nakon toga se pokreće ažuriranje te skeniranje uređaja. Nakon toga je potrebno napraviti Mcafee račun kako bi nam bile omogućene sve funkcionalnosti koje se nalaze u besplatnoj verziji aplikacije.

Funkcionalnosti koje se nalaze na početnom zaslonu jednostavno su raspoređene jedna ispod druge, a na vrhu ekrana se nalazi tipka sa obavijestima te profil sa kojim je korisnik prijavljen.

Klikom na jednu od 6 ponuđenih funkcionalnosti ulazi se u podizbornik svake.

Slika 5.26. Početni zaslon McAfee aplikacije

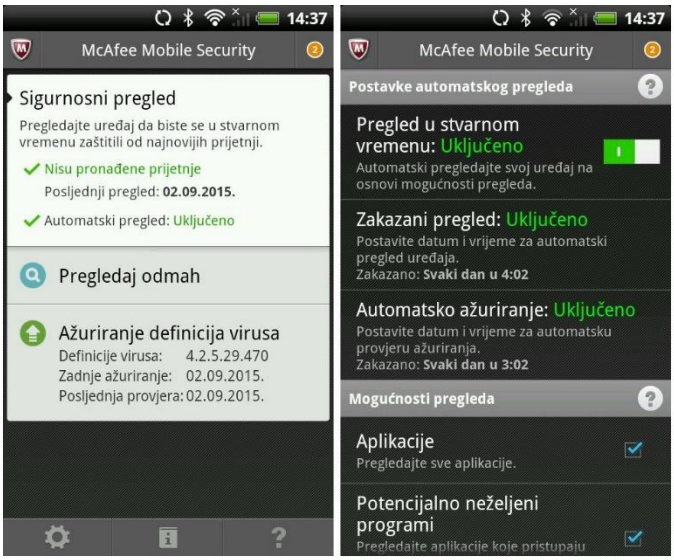
. U svakom podizborniku na dnu ekrana se nalaze tri tipke (postavke, vodič i pomoć) koje korisnik prema potrebi koristi.

5.4.2. Funkcionalnosti Mcafee aplikacije

Funkcionalnosti McAfee aplikacije možemo podijeliti u 6 kategorija, a to su:

- Sigurnosni pregled,
- Privatnost,
- Optimizator baterije,
- Traženje uređaja,
- Sigurnosno kopiranje,
- Web sigurnost

Sigurnosni pregled koristi se kako bi se uređaj u stvarnom vremenu zaštitio od najnovijih prijetnji. Unaprijed je postavljen automatski pregled uređaja prema rasporedu, no uvijek se mogu prilagoditi postavke pregleda u skladu sa željama korisnika.

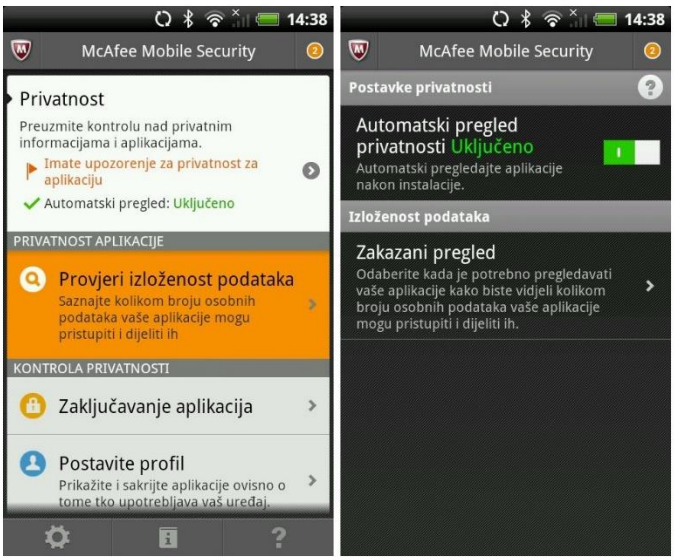


Slika 5.27. Podizbornik sigurnosnog pregleda

Ulaskom u podizbornik korisniku se pri dnu ekrana nude tri opcije (postavke, info i pomoć). Klikom na tipku postavke korisnik može prilagoditi postavke svojim potrebama, uključiti automatsko pregledavanje uređaja, odrediti vrijeme i datum automatskog pregleda ili može dopustiti Pametnom planeru da odredi najbolje vrijeme. Korisnik može odrediti i mogućnosti pregleda, pregledavanje instaliranih aplikacija, onih aplikacija koje pristupaju privatnim podacima, pregled tekstualnih i multimedijalnih poruka te svih datoteka na uređaju uključujući SD karticu.

Privatnost je funkcionalnost koja se odnosi na pregledavanje aplikacija na uređaju te izvještavanje o vrsti informacija kojima aplikacije pristupaju i koje dijele te omogućavaju korisniku da blokira njihov pristup značajkama kao što je fotoaparat, kontakt ili lokacija. Također omogućeno je zaključavanje i skrivanje aplikacija kada se uređaj dijeli s obitelji i prijateljima. Mcafee Mobile Security ocjenjuje aplikacije korisnika na temelju količine osobnih podataka kojima pristupaju i koje dijele.

Moguće je uključiti automatski pregleda aplikacija nakon instalacije te odrediti kada je potrebno pregledavati aplikacije kako bi se vidjelo kolikom broju osobnih podataka instalirane aplikacije mogu pristupiti i dijeliti ih, na dnevnoj ili tjednoj bazi.



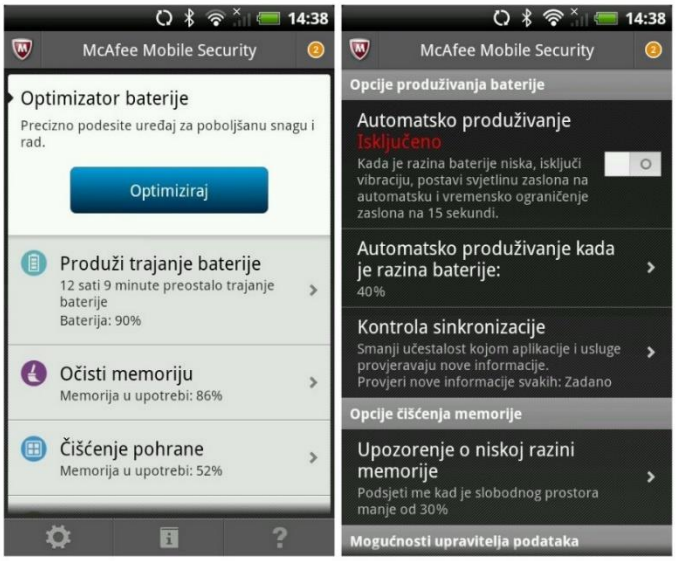
Slika 5.28. Podizbornik privatnosti

Optimizator baterije koristi se kako bi se uređaj podesio za poboljšanu snagu i rad. Klikom na tipku optimiziraj automatski će se produžiti vijek trajanja baterije, osloboditi memorija i očistiti pohrana kako bi uređaj učinkovitije radio.

Funkcionalnost omogućuje korisnicima uvid koliko koja aplikacija i senzori uređaja troše bateriju, provjeriti kolika je ušteda baterije isključivanjem aplikacija i senzora, postaviti automatski prag kako se baterija ne bi potrošila kada je najviše potrebna. Korisnici mogu i samo pokrenuti čišćenje memorije, produženje trajanja baterije, čišćenje pohrane ili pratiti uporabu podataka zasebno.

Također moguće je postaviti automatsko produživanje kada je razina baterije niska, tada će se isključiti vibracije, postaviti svjetlina zaslona na automatsko i vremensko ograničenje na 15 sekundi. Kontrolu sinkronizacije tj. učestalost kojom aplikacije i usluge provjeravaju nove informacije mogu se postaviti na 30 minuta, 1h, 2h i zadano.

Kod opcija čišćenja memorije može se podesiti na kojem postotku popunjenosti memorije da se pojavi upozorenje (15%, 20% ili 30 %). Korisnik može ograničiti potrošnju podataka, te namjestiti obavijest nakon potrošene određene količine podataka.



Slika 5.29. Podizbornik optimiziranja baterije

Traženje uređaja kao što i sam naziv govori omogućuje pronalazak uređaja tj. njegovo lociranje na karti, zaključavanje, izradu sigurnosnih kopija, ili čišćenja zbog zaštite bitnih informacija.

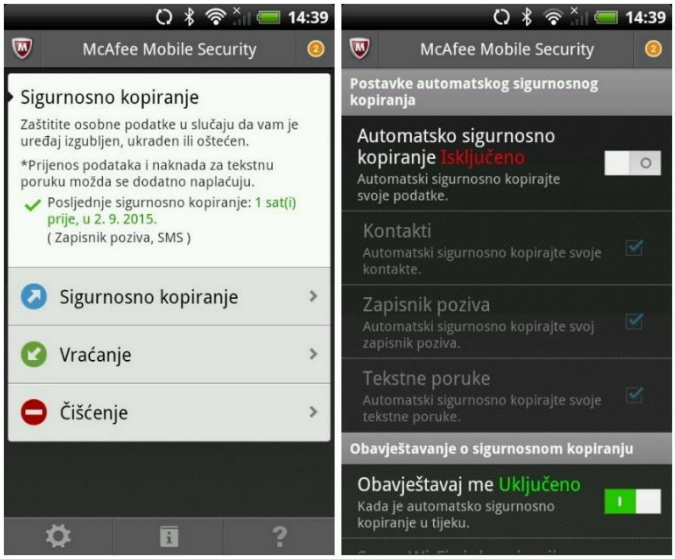
Slika 5.30. Podizbornik traženja uređaja

Ukoliko je mobilni uređaj izgubljen, prijavom na web-račun Mcafee Mobile Security-a može ga se locirati i pratiti na karti. Ukoliko je baterija pri kraju, S.O.S. značajka pokazuje zadnju poznatu lokaciju uređaja prije nego što se isključi. Prije upotrebe ove funkcionalnosti potrebno je uključiti GPS ili lokacije u postavkama svog uređaja.

Ukoliko korisnik ostavlja mobilni uređaj na mjestu koje nije sigurno može ga zaključati da bi zaštitio osobne podatke na njemu.

Traženje uređaja se još nudi aktiviranje alarma ukoliko se uređaj nalazi u blizini, a korisnik ga ne može pronaći, aktivira se alarm koji olakšava pronalazak. Zaštita od deinstalacije otežava lopovima deinstaliranje ove aplikacije tako da privatni korisnički podaci ostaju privatni čak i kada je uređaj izgubljen ili ukraden. Ako se aktivira opcija deinstaliranja, ova aplikacija se može ukloniti isključivo s pomoću administratora uređaja i valjanog PIN-a za Mcafee Mobile Security.

Sigurnosno kopiranje omogućava spremanje tekstualnih poruka, zapisnik poziva, kontakata te prijenos medija (u Premium verziji) te vraćanje tekstualnih poruka i kontakata koji su u nekom trenutku bili sigurnosno kopirani.



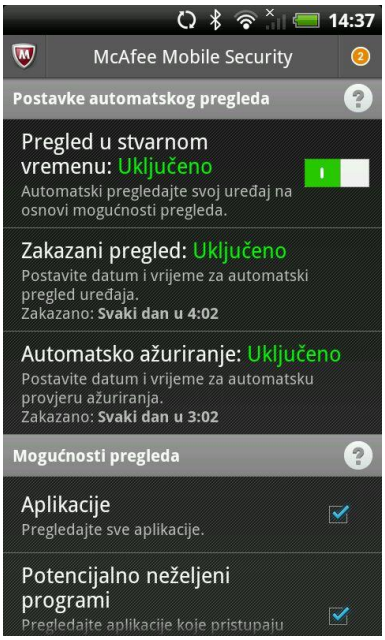
Slika 5.31. Podizbornik sigurnosnog kopiranja

Kao što je vidljivo na slici 45. korisnik sam odlučuje koji će se podaci sigurnosno kopirati te hoće li se to kopiranje odvijati automatski ili će ga sam pokretati. Može odrediti hoće li biti obavješten kada je automatsko sigurnosno kopiranje u tijeku. Bilo bi dobro da se sigurnosno kopiranje, vraćanja i prijenosa izvodi kada je korisnik spojen na Wi-Fi mrežu kako ne bi došlo do dodatne naplate.

Web sigurnost će reći korisniku koja su web-mjesta, veze i Wi-Fi mreže sigurne, a koje nisu kako bi se mogli povezivati na mrežu, surfati i pretraživati bez straha.

5.4.3. Otkrivanje sigurnosnih prijetnji i performanse

Skeniranje se pokreće u izborniku Sigurnosni pregled, moguće je postaviti skeniranje svih aplikacija, skeniranje potencijalno neželjenih programa ili skeniranje svih file-ova koji se nalaze u internoj memoriji uređaja ili vanjskoj memoriji.



Slika 5.32. Podizbornik sigurnosnog pregleda

Moguće je podesiti zakazano skeniranje svaki dan ili u određeno vrijeme u tjednu. Mcafee nudi i "Pametno skeniranje" koje odabire najbolje vrijeme za skeniranje uređaja najčešće kada ga korisnik ne koristi.

5.5. Norton Mobile Security

Norton ili kako se još naziva Norton by Symantec razvijen je od strane Petera Nortona čija se tvrtka Peter Norton Computing 1990. godine priključila grupaciji Symantec. Norton Mobile security sprječava i uklanja zlonamjerni sadržaj sa mobilnog uređaja.

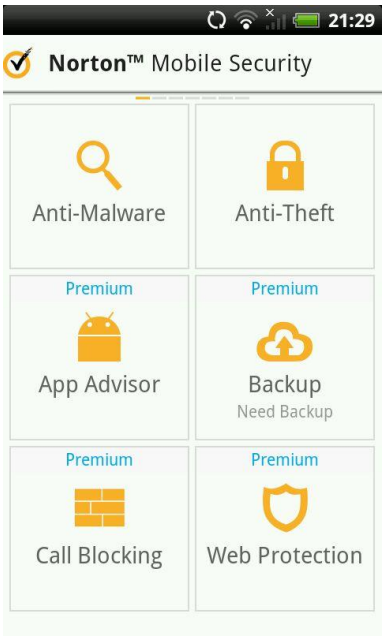
Početkom 1991. godine lansiran je prvi antivirusni program za PC, Norton AntiVirus 1.0. Posljednjih desetljeća tvrtka unapređuje svo je proizvode te tako najnovija linija proizvoda uključuje Norton Security, Norton Small Business, Norton Family, Norton Mobile Security, Norton Online Backup, Norton360, Norton Utilities.

Norton Mobile Security dolazi u dvije verzije, besplatnoj i Premium iako se instaliranjem besplatne verzije dobivaju Premium funkcionalnosti na 30 dana.

Sastoji se od šest funkcionalnosti koje će kasnije biti opisane, a tu su Anti-Malware koje se jedine nalaze u besplatnoj verziji, ostale četiri funkcionalnosti se mogu koristiti prvih 30 dana ili nakon nadogradnje na Premium verziju, to su App Advisor, Backup, Call Blocking i Web Protection.

5.5.1. Podešavanje Norton Mobile Security aplikacije

Norton Mobile Security aplikacija preuzeta je s Google Play trgovine, veličine je 7.75 MB, preuzeta verzija je besplatna te ima više od 10 milijuna preuzimanja.



Slika 5.33. Izbornik Norton Mobile Security-a

Nakon instaliranja aplikacije potrebna je izrada računa kako bi se mogle koristiti sve funkcionalnosti aplikacije. U odnosu na ostale aplikacije koje se koriste u istraživanju, Norton Mobile Security ima najjednostavnije sučelje za korištenje.

Početni zaslon je podijeljen na 6 funkcionalnosti. Klikom na pojedinu funkcionalnost otvara izbornik iste. Funkcionalnosti se osim klikom na početnom zaslonu mogu koristiti i klizanjem ekrana lijevo ili desno. Klikom na tipku *menu* na uređaju HTC Desire Hd na kojem se radilo istraživanje, otvara se izbornik koji nudi skeniranje, postavke, dnevnik aktivnosti, podjela aplikacije, pomoć, informacije o samoj aplikaciji i ponuda drugih Nortonovih aplikacija.

Funkcionalnosti pokraj kojih se nalazi natpis Premium se nakon početnih 30 dana ne mogu koristiti ukoliko korisnik ne nadogradi besplatnu verziju Premium verzijom koja se plaća 29,99 eura godišnje ili u nekom od paketa koji nudi Norton Security.

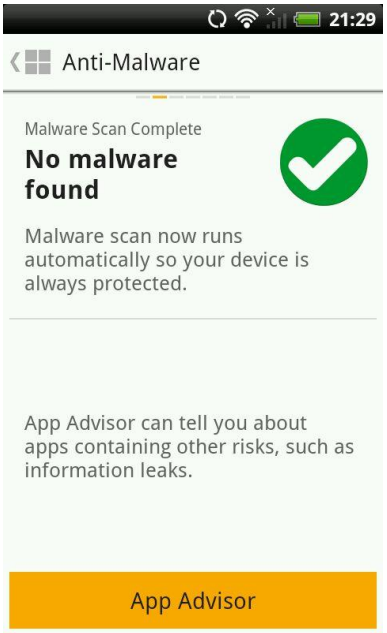
5.5.2. Funkcionalnosti Norton Mobile Security aplikacije

Kao što je u prošlom pod poglavlju navedeno, funkcionalnosti koje su dostupne u Norton Mobile su:

- Anti-Malware,
- Anti-Theft,
- App Advisor,
- Backup,
- Call Blocking i
- Web Protection

Anti-Malware se koristi za skeniranje mobilnog uređaja. Klikom na gumb Anti-*Malware* dobivamo uvid u pronađene *malware* te možemo pokrenuti App Advisor.

Ukoliko želimo pokrenuti skeniranje mobilnog uređaja, potrebno je kliknuti na *menu* tipku uređaja i pokrenuti skeniranje. Dodatne postavke skeniranja kao što su vrijeme skeniranja i opcija što će se skenirati potrebno je kliknuti *menu* tipku uređaja i nakon toga na postavke.



Slika 5.34. Podizbornik Anti-Malware

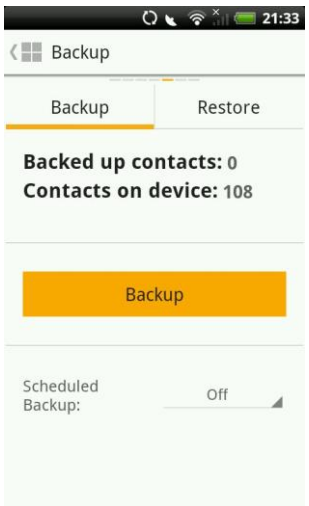
Sljedeća funkcionalnost je **Anti-Theft** kojom koristeći SMS ili Web možemo udaljenim putem zaključati uređaj, uključiti alarm, locirati uređaj, uslikati trenutnog korisnika mobilnog uređaja ukoliko mobilni uređaj ima prednju kameru ili pobrisati podatke sa uređaja.

Ukoliko korisnik želi promijeniti postavke ove funkcionalnosti može to učiniti klikom na tipku *menu* uređaja te nakon toga na tipku postavke.

Slika 5.35. Anti-Theft funkcionalnost

App Advisor daje korisniku informacije o potencijalnim opasnostima pojedinih aplikacija, npr. gubitak privatnih podataka. Također javlja korisniku informacije o povećanoj potrošnji baterije ili podataka. App Advisor ne nudi dodatne postavke koje korisnik može mijenjati.

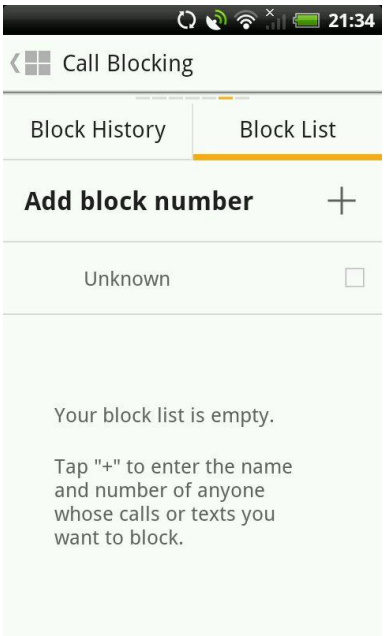
Backup omogućava sigurnosno kopiranje kontakata i vraćanje istih, moguće je postaviti automatsku izradu sigurnosnih kopija dnevno, tjedno, i mjesečno.



Slika 5.36. Podizbornik Backup-a

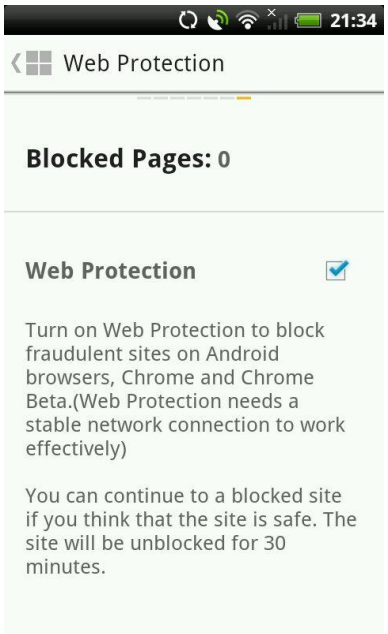
Peta funkcionalnost je **Call blocking**, ulaskom u podizbornik moguće je pregledati povijest blokiranih poziva i SMS-ova te dodati broj od kojih se želi blokirati pozive i SMS-ove također moguće je blokirati i pozive nepoznatih brojeva.

Call blocking funkcionalnost spada u Premium funkcionalnosti Norton Mobile Securty aplikacije ali je 30 dana dostupna besplatno u probnom razdoblju.



Slika 5.37. Podizbornik Call Blockinga

Posljednja funkcionalnost je **Web zaštita** koja blokira web stranice koje na prijevaru pokušavaju doći do korisničkih podataka ili zaraziti korisnički uređaj sa zlonamjernim sadržajem. Blokiranje se može ostvariti na Android pretraživačima, Chrome i Chrome beta pretraživačima. Web konekcija mora imati stabilnu mrežnu vezu kako bi radila efektivno.



Slika 5.38. Podizbornik Web zaštite

Podizbornik web zaštite ne nudi dodatne postavke kao što su nudili neki od prije opisanih antivirusnih alata.

5.5.3. Otkrivanje sigurnosnih prijetnji i performanse

Anti-Malware funkcionalnost koja se koristi za skeniranje aplikacija instaliranih na uređaju nema dodatne opcije osim određivanja kada će se skeniranje obaviti, može biti isključeno ili se može namjestiti dnevno, tjedno ili mjesečno skeniranje, moguće je još odrediti hoće li se skenirati SD kartica ukoliko se nalazi u uređaju.

6. Komparativna analiza antivirusnih alata

U ovom poglavlju biti će opisano istraživanje, komparativna analiza antivirusnih alata. Koristilo se pet antivirusnih alata za Android uređaj i jedan antivirusni alat za iOS uređaj. Alati koji su se koristili u istraživanju su Lookout za iOS i Android uređaj te Avast Mobile Security, Trend Micro Mobile Security, Mcafee Mobile Security, Norton Mobile Security za Android uređaj.

Korištene su besplatne verzije antivirusnih alata, a pojedini alati su imali uključene i Premium funkcionalnosti u prvih 30 dana korištenja. Za iOS uređaj korišten je samo jedan antivirusni alat jer su uvjeti bili da antivirusni alat ima besplatnu verziju, mogućnost skeniranja aplikacija, da bude kompatibilan sa verzijom 6 iOS operativnog sustava. te da postoji ista verzija za Android operativni sustav.

5.2. Korišteni mobilni terminalni uređaji

Uređaji koji su se koristili u istraživanju su HTC Desire HD sa Android operativnim sustavom i Apple iPhone 3GS sa iOS operativnim sustavom.

Za početak rada s uređajem Apple iPhone 3gs potrebna je aktivacija koju nije moguće napraviti bez umetanja SIM kartice u uređaj. U uređaj je umetnuta SIM kartica mobilnog operatera VIP. Izrađen je Apple ID. Napravljen je *reset* postavki i sadržaja te je ažuriran softver sa verzije iOS 3.0 na verziju iOS 6.1.6 (71.8 MB). SIM kartica je potrebna samo za aktivaciju uređaja, nakon aktivacije se može izvaditi i uređaj se može koristiti bez SIM kartice.

Andorid uređaj koji će se koristit u istraživanju je HTC Desire HD. Za aktivaciju uređaja nije potrebna SIM kartica. Aktivacija uređaja je obavljena prijavom na Google račun, spajanjem na bežičnu mrežu Fakulteta prometnih znanosti LSF. Napravljen je *factory reset* uređaja te je ažuriran softver sa verzije Android OS 2.2 (Froyo) na verziju Android OS 2.3.5 (Gingerbread).

NETWORK	Technology	GSM / HSPA
	2G bands	GSM 850 / 900 / 1800 / 1900
	3G Network	HSDPA 900 / 2100
		HSDPA 850 / 1900 - North America
	Speed	HSPA 14.4/5.76 Mbps or HSPA 7.2/2 Mbps (carrier dependent)
	GPRS	Class 32
	EDGE	Class 32
LAUNCH	Announced	2010, September
	Status	Available. Released 2010, October
BODY	Dimensions	123 x 68 x 11.8 mm (4.84 x 2.68 x 0.46 in)
	Weight	164 g (5.78 oz)
	SIM	Mini-SIM
DISPLAY	Type	LCD capacitive touchscreen, 16M colors
	Size	4.3 inches (~62.9% screen-to-body ratio)
	Resolution	480 x 800 pixels (~217 ppi pixel density)
	Multitouch	Yes
	Protection	Corning Gorilla Glass
		- HTC Sense UI
PLATFORM	OS	Android OS, v2.2 (Froyo), v2.3 (Gingerbread), not upgradable to v4.0 (Ice Cream Sandwich)
	Chipset	Qualcomm MSM8255 Snapdragon S2
	CPU	1 GHz Scorpion
	GPU	Adreno 205
MEMORY	Card slot	microSD, up to 32 GB, 8 GB included
	Internal	1.5 GB; 768 MB RAM
CAMERA	Primary	8 MP, 3264 x 2448 pixels, autofocus, dual-LED flash
	Features	Geo-tagging, face detection
	Video	720p
	Secondary	No
SOUND	Alert types	Vibration; MP3, WAV ringtones
	Loudspeaker	Yes
	3.5mm jack	Yes
		- Dolby Mobile, SRS sound
COMMS	WLAN	Wi-Fi 802.11 b/g/n, DLNA, hotspot
	Bluetooth	v2.1, A2DP
	GPS	Yes, with A-GPS
	Infrared port	No
	Radio	Stereo FM radio with RDS
	USB	microUSB v2.0
FEATURES	Sensors	Accelerometer, proximity, compass
	Messaging	SMS(threaded view), MMS, Email, Push Email, IM
	Browser	HTML, Adobe Flash
	Java	Yes, via Java MIDP emulator
		- Dedicated search key - MP3/AAC+/WAV/WMA9 player - DivX/Xvid/MP4/H.264/WMV9/player - Voice memo - Predictive text input
BATTERY		Li-Ion 1230 mAh battery
	Stand-by	Up to 490 h (2G) / Up to 420 h (3G)
	Talk time	Up to 9 h 15 min (2G) / Up to 5 h 30 min (3G)

Slika 6.2. Specifikacije HTC Desire HD uređaja, [21]

Slika 6.1. HTC Desire HD uređaj

Sa lijeve strane na slici 54. mogu se vidjeti karakteristike mobilnog uređaja HTC Desire HD-a koji je korišten u istraživanju.

NETWORK	Technology	GSM / HSPA
	2G bands	GSM 850 / 900 / 1800 / 1900
	3G Network	HSDPA 850 / 1900 / 2100
	Speed	HSPA 7.2/0.384 Mbps
	GPRS	Yes
	EDGE	Yes
LAUNCH	Announced	2009, June. Released 2009, June
	Status	Discontinued
BODY	Dimensions	115.5 x 62.1 x 12.3 mm (4.55 x 2.44 x 0.48 in)
	Weight	135 g (4.76 oz)
	SIM	Mini-SIM
DISPLAY	Type	TFT capacitive touchscreen, 16M colors
	Size	3.5 inches (~50.9% screen-to-body ratio)
	Resolution	320 x 480 pixels (~165 ppi pixel density)
	Multitouch	Yes
	Protection	Corning Gorilla Glass, oleophobic coating
PLATFORM	OS	iOS 3, upgradable to iOS 6.1.3
	Chipset	
	CPU	600 MHz Cortex-A8
	GPU	PowerVR SGX535
MEMORY	Card slot	No
	Internal	8/16/32 GB, 256 MB RAM
CAMERA	Primary	3.15 MP, 2048 x 1536 pixels, autofocus
	Features	Geo-tagging, touch focus
	Video	480p@30fps
	Secondary	No
SOUND	Alert types	Vibration, proprietary ringtones
	Loudspeaker	Yes
	3.5mm jack	Yes
COMMS	WLAN	Wi-Fi 802.11 b/g
	Bluetooth	v2.1, A2DP (headset support only)
	GPS	Yes, with A-GPS
	Infrared port	No
	Radio	No
	USB	v2.0
FEATURES	Sensors	Accelerometer, proximity, compass
	Messaging	iMessage, SMS (threaded view), MMS, Email
	Browser	HTML (Safari)
	Java	No
		- iCloud cloud service - Maps - Organizer - TV-out - Audio/video player/editor - Photo viewer/editor - Voice command/dial - Predictive text input
BATTERY		Non-removable Li-Ion battery
	Stand-by	Up to 300 h
	Talk time	Up to 12 h (2G) / Up to 5 h (3G)

Slika 6.4. Specifikacije Apple iPhone 3GS-a

Slika 6.3. Apple iPhone 3GS

Sa lijeve strane na slici 56. mogu se vidjeti karakteristike Apple iPhone 3GS uređaja koji je korišten u istraživanju.

5.3. EICAR test

EICAR standardna antivirusna testna datoteka ili EICAR testna datoteka, je računalna datoteka razvijena od strane EICAR-a (European Institute for Computer Antivirus Research – Europski institut za istraživanje zaštite od računalnih virusa) i organizacija CARO-a (Computer Antivirus Reasearch Organization - Istraživačka organizacija računalnih antivirusa) da bi se testirao odziv računalnih antivirusa. Umjesto korištenja pravih *malware*-a koji mogu oštetiti računalo ili mobilni uređaj, ova datoteka omogućava korisnicima da testiraju antivirusne programe bez upotrebe pravih virusa.

Korištenje EICAR testa trebalo bi odgovoriti na pitanja poput:

- je li antivirusni program instaliran ispravno, ako je pronalazi li i/ili briše viruse kao što bi trebao
- što se događa kada antivirusni program detektira virus
- koja se poruka tada javlja korisniku

Ideja je da antivirusni program detektira testnu datoteku na način kao da se rado o virusu i tako je tretira, [22].

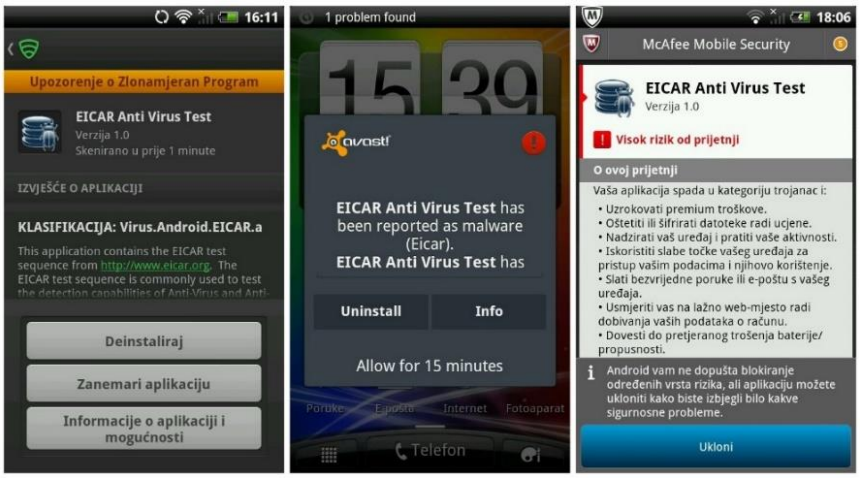
EICAR datoteka je kratka i jednostavna, sastoji se isključivo od ASCII znakova, tako da može lako biti kreiran sa jednostavnim alatom za uređivanje teksta. Za primjer možemo uzeti jednostavan blok za pisanje u koji trebamo upisati sljedeće znakove i spremili sa nastavkom .com.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Za testiranje antivirusnih alata, korištena je EICAR Anti-virus Test aplikacija koja sadrži EICAR datoteku, aplikacija je u potpunosti bezopasna. EICAR Anti-virus Test aplikacija preuzeta je sa Google Play trgovine, veličine je 17,50 kB te ima više od 100 000 preuzimanja. Prije svakog testiranja različitog antivirusnog alata, uređaj je vraćen na tvorničke postavke.

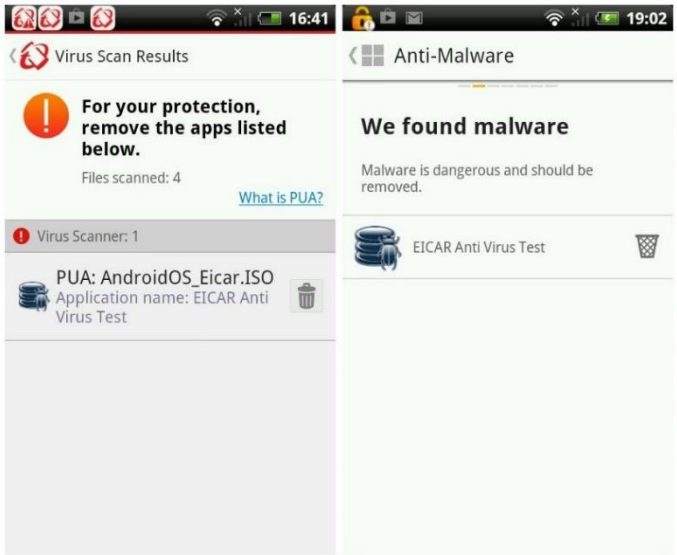
Svi antivirusni alati korišteni na Andorid operativnom sustavu su prepoznali EICAR datoteku kao *malware*. Na mobilni terminalni uređaj sa iOS operativnim sustavom je preuzeta EICAR datoteka sa web stranice http://www.eicar.org/ , ali ga aplikacija Lookout ne prepoznaje kao prijetnju.

Slika 6.5. prikazuje prepoznavanje EICAR datoteke kao *malware*-a u aplikacijama Lookout, Avast Mobile Security i McAfee Mobile Security.



Slika 6.5. Lookout, Avast i McAfee prepoznaju EICAR datoteku kao malware

Na slici 6.6 može se vidjeti prepoznavanje EICAR datoteke kao *malware*-a u Trend Micro mobilnoj aplikaciji.



Slika 6.6. Trend Micro Mobile Security i Norton Mobile Security prepoznaju EICAR datoteku kao malware

5.4. Najposjećenije Web stranice u Hrvatskoj

U ovom poglavlju biti će opisano testiranje 50 najposjećenijih Web stranica u Hrvatskoj. Postoji velik broj agencija koje se bave prikupljanjem podataka i rangiranjem stranica, neke ne nude javno dostupne informacije ukoliko vlasnik web stranice to ne želi npr. Google Analytics, neke se plaćaju, a neke su izbacile određene web portale iz svojih mjerenja zbog nedozvoljenih radnji kako bi povećale broj posjetitelja. Također može biti slučaj kada vlasnici web stranica ne žele sudjelovati u statistici pa je onda teško napraviti relevantnu listu najposjećenijih stranica te one variraju.

Prednost odabrane statistike tvrtke Alexa je što velik dio svojih statističkih podataka objavljuje javno, nedostatak je što broj prikazanih posjetitelja ovisi o postotku posjetitelja koji koriste Alexa alatnu traku ili Internet Explorer zbog čega su moguća odstupanja od realnih podataka.

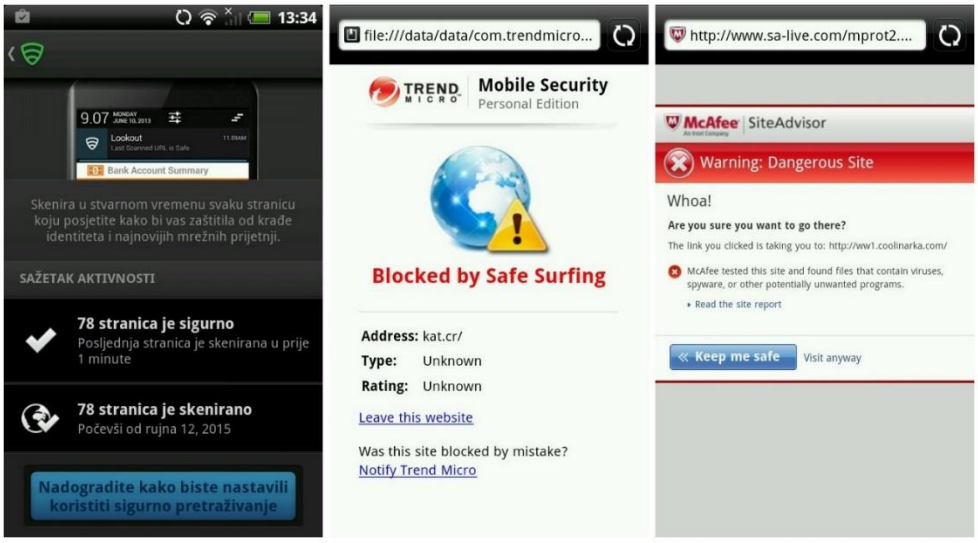
Alexa tvrtka koja se bavi prikupljanjem komercijalnih podataka o web prometu, podružnica je kompanije Amazon. Osnovana je kao nezavisna kompanija 1996. godine, ali ju je 1999. godine kupila kompanija Amazon. Procjena prometa Alexe temelje se na podacima iz njihove globalne prometne ploče koja je uzorak od milijuna korisnika interneta koristeći jedan od preko 25 tisuća različitih proširenja preglednika. Osim toga velik dio prometnih podataka skupljaju iz direktnih izvora sa forme web stranica čiji su korisnici odlučili instalirati Alexa

skripte na njihovim stranicama i potvrditi svoje podatke. Vlasnici mogu uvijek odlučiti žele li da ti podaci budu javni ili privatni. U nastavku u Tablici 6.1 nalazi se lista najposjećenijih web stranica prema Alexa statistici.

Tablica 6.1. 50 najposjećenijih web stranica u Hrvatskoj

1. Google.hr	11. Dnevnik.hr	21. Telegram.hr	31.Dnevno.hr	41.Wordpress.com
2. Facebook.com	12. Wikipedia.org	22. Blogspot.com	32.Prognoza.hr	42.Coolinarka.com
3. Google.com	13. Yahoo.com	23. Rtl.hr	33.Moj-posao.hr	43.Hrt.hr
4. Youtube.com	14. Tportal.hr	24. Linkedin.com	34.Lika-online.com	44.Paypal.com
5. Jutarnji.hr	15. Amazon.com	25. Aliexpress.com	35.Imgur.com	45.Xhamster.com
6. Index.hr	16. Slobodnadalmacija.hr	26. Diply.com	36.Kat.cr	46.Reddit.com
7. Njuskalo.hr	17. Ebay.com	27. Booking.com	37.Pornhub.com	47.Xvideos.com
8. 24sata.hr	18. Forum.hr	28. Live.com	38.Novilist.hr	48.Pbz.hr
9. Vecernji.hr	19. Twitter.com	29. Onclickads.net	39.Rezultati.com	49.Ask.com
10. Net.hr	20. Imdb.com	30. Instagram.com	40.Google.de	50.Pintrest.com

Od testiranih antivirusnih alata jedino Avast Mobile Security aplikacija nema funkcionalnost provjere sigurnosti web stranice koja se pretražuje. Na slici 60. mogu se vidjeti rezultati pretraživanja 50 najposjećenijih web stranica u Hrvatskoj.



Slika 6.7. Izvješće o sigurnosti web stranica pojedinih antivirusnih alata

Lookout antivirusni program nije niti jednu stranicu označio kao potencijalnu prijetnju. Trend Micro Mobile Security nudi tri razine filtriranja potencijalnih prijetnji, na razinama *Low*

i *Normal* nije bilo obavijesti o prijetnjama dok je razina *High* označila web stranicu Kat.cr (KickassTorrents) kao potencijalnu prijetnju, stranica se koristi za dijeljenje datoteka koristeći se BitTorrent protokol i najposjećenija je stranica tog tipa prema statistici Alexa agencije. Također Trend Micro Mobile Security kao potencijalnu prijetnju označio je i reklame koje se pojavljuju na stranicama sa sadržajem za odrasle Pornhub.com, Xhamster.com i Xvideos.com.

McAfee Mobile Security je kao potencijalnu prijetnju označio web stranicu Coolinarka.com te reklame na stranici sa sadržajem za odrasle Xvideos.com. Norton Mobile Security nije označio niti jednu web stranicu kao potencijalnu prijetnju. Lookout antivirusni alat na iOS uređaju također nije zabilježio nikakve potencijalne prijetnje na navedenim stranicama .

5.5. Testiranje uzorcima malware-a

Uzorci *malware*-a koji su korišteni u testiranju su preuzeti sa web stranice contagiodump.blogspot.com. Stranicu čine najnoviji uzorci raznih *malware*-a, prijetnji, promatranja i analiza.

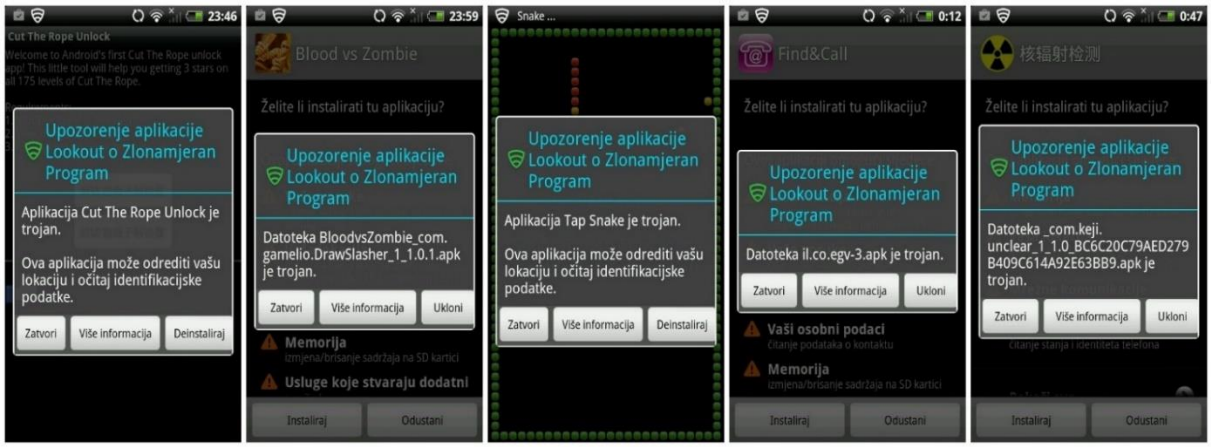
Za testiranje se koristilo 5 *malwarea* sa navedene stranice koji su preuzeti na računalo te prebačeni na testirani uređaj HTC Desire HD kablom. Moguće je i direktno preuzimanje na mobilni uređaj ali je zbog praktičnosti izvođenja testiranja sadržaj preuzet prvo na računalo. Preuzeti *malware* je pohranjen u zip formatu tako da je bilo potrebno instalirati zip čitač na uređaj kako bi se mogle „raspakirati“ datoteke i pokrenuti. Ovaj dio se može odraditi i na računalu pa se na mobilni uređaj prebacuje samo APK datoteka aplikacije.

Popis *malware*-a koji se koristio kod testiranja antivirusnih alata:

1. **DroidKungFu2 -A** _com.allen.txthej_1_1.0F438ED38B59F772E03EB2CAB97FC7685
2. **GoldDream.A** BloodvsZombie_com.gamelio.DrawSlasher_1_1.0.1.apk b87f2f3a927bf9677 36ed43ca2dbfb60
3. **net.maxicom.android.snake** 7937c1ab615de0e71632fe9d59a259cf
4. **Android FindAndCall** spyware
5. **Basebridge A_com.keji.unclear_1_1.0.apk** BC6C20C79AED279B409C614A92E63BB9

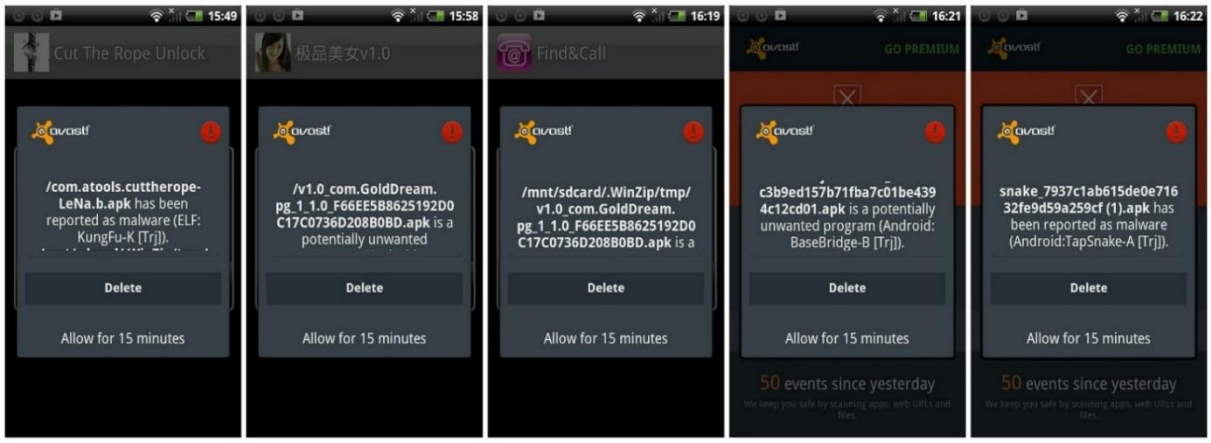
Kod svakog pokretanja aplikacije bilo je potrebno upisati lozinku, za sav sadržaj sa Contagiodump stranice koji se preuzima potrebno je upisati lozinku koja se nalazi uz naziv datoteke ili je potrebno kontaktirati osobu koja je prenijela sadržaj na stranicu.

Prilikom prepoznavanja instaliranog *malware*-a, Lookout aplikacija omogućuje korisniku da zanemari upozorenje, sazna više informacija o otkrivenom zlonamjernom programu ili da ga odmah ukloni, ukoliko korisnik ne ukloni *malware* odmah, može ga ukloniti kasnije ulaskom u Lookout aplikaciju.



Slika 6.8. Lookout prepoznaje instalirani malware

Avast Mobile Security omogućuje korisniku da i dalje koristi *malware* odnosno zaraženu aplikaciju narednih 15 minuta nakon kojih će se ponovno pojaviti na ekranu upozorenje ili da izbriše zlonamjerni sadržaj odmah.

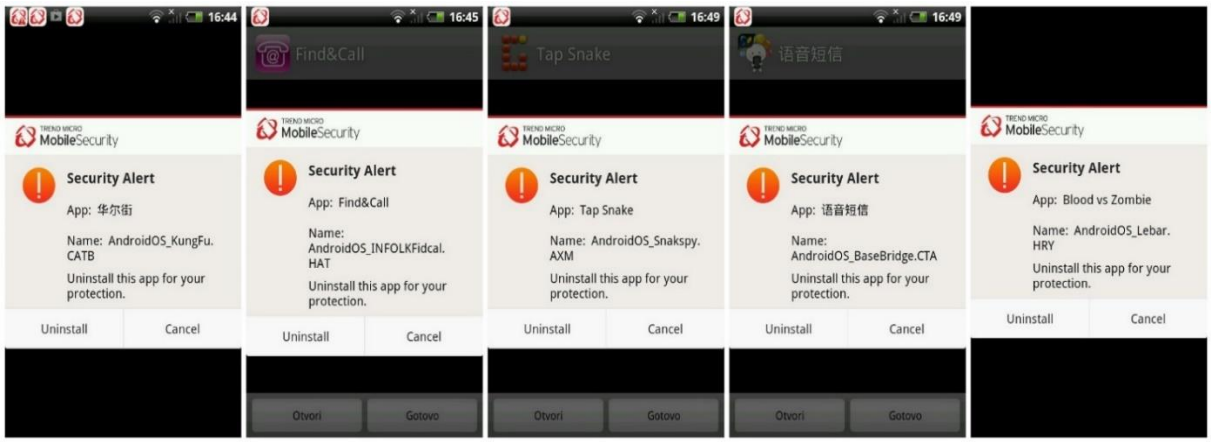


Slika 6.9. Avast prepoznaje instalirani malware

Trend Micro Mobile Security osim upozorenja za instalirani *malware*-a upozorava i na čitač zip formata WinZip koji je preuzet sa Google Play trgovine.

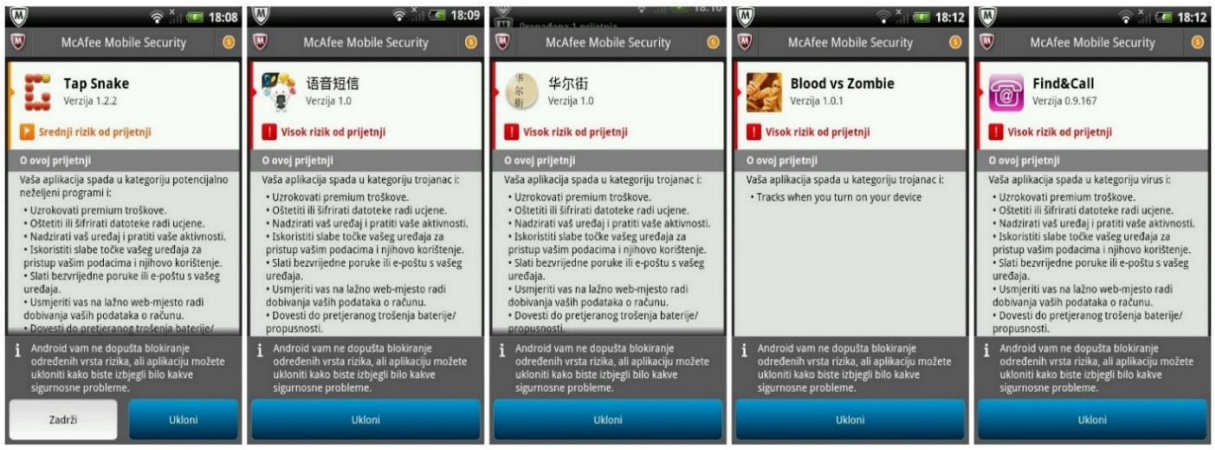
Upozorenje se odnosi na potencijalno narušavanje privatnosti jer aplikacija prikuplja podatke o jedinstvenom broju uređaja, državi u kojoj se korisnik nalazi te informacije o mrežnom operateru.

Ostali antivirusni alati korišteni u istraživanju nisu označile WinZip aplikaciju kao potencijalnu prijetnju.



Slika 6.10. Trend Micro prepoznaje instalirani malware

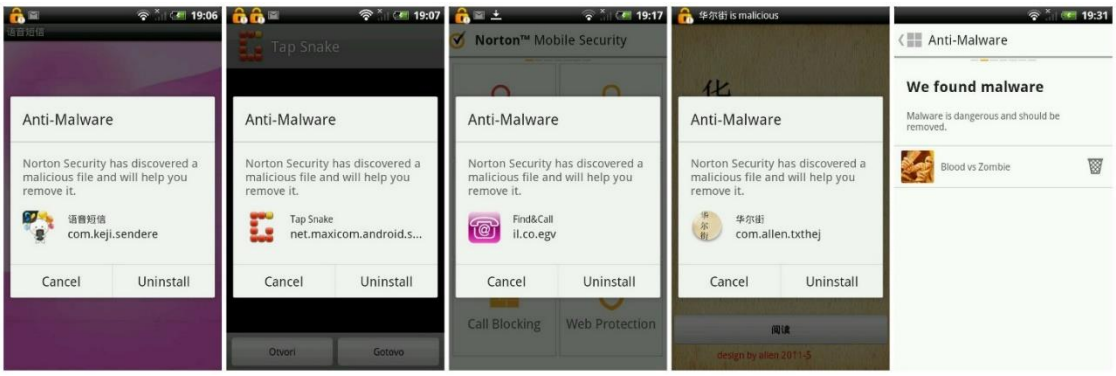
McAfee Mobile Security je također prepoznao sve *malware* te čak ima klasifikaciju prijetnji. Tap Snake aplikaciju je označio kao srednju razinu prijetnje, a ostale četiri kao visoku razinu prijetnje.



Slika 6.11. McAfee prepoznaje instalirani malware

Uz obavijest o pojavi potencijalne prijetnje McAfee nudi i detaljne informacije o šteti koju može prouzročiti *malware*.

Norton Mobile Security nakon otkrivanja zlonamjernog sadržaja omogućava korisniku nastavak korištenja aplikacije ili deinstaliranje aplikacije odmah u trenutku javljanja upozorenja.



Slika 6.12. Norton prepoznaje instalirani malware

Android operativni sustav zasnovan je na Linux software te je sličan Linux operativnom sustavu, otvoreniji je sustav od iOS operativnog sustava te je besplatan, dopušta instaliranje aplikacija treće strane odnosno aplikacije koje se ne nalaze na službenoj Google Play trgovini. Korisnik može sam dopustiti ili ne dopustiti instaliranje aplikacija iz nepoznatih izbora u postavkama samog uređaja na vlastitu odgovornost. Prema istraživanju Pulse Secure-a 97% *malwarea* je otkriveno na Android operativnom sustavu.

Iako se za iOS operativni sustav zna reći da nema virusa, proteklih godina se pojavilo nekoliko virusa (za uređaje koji nisu otključani) koji su u kratko vremenu uklonjeni dok je otključane uređaje bilo nešto više virusa.

Otključavanjem uređaja korisnici imaju mogućnost instaliranja aplikacija i sadržaja trećih strana, ali su time izloženi riziku. Ukoliko se uređaj ne otključa tj. *jailbreaka*, rizik „zaraze“ uređaja zlonamjernim sadržajem je minimalan.

U tablici 6.2 prikazana su tri virusa koji su pronađeni na zaključanim iPhone uređajima, na otključanim uređajima broj virusa je nešto viši, desetak pronađenih virusa.

WireLurker je virus koji se pojavio 2014. godine, virusu je bio cilj instaliranje aplikacija na iOS uređaje, najveći problem su imali korisnici u Kini koji koriste dodatne trgovine za instaliranje aplikacija (Maiyadi App store) također virus se prenosi i spajanjem iOS uređaja na OS X operativni sustav. Čak i u ovom slučaju korisnici van Kineskog tržišta nisu toliko ugroženi ukoliko ne instaliraju sadržaj sa neslužbenih Apple trgovina, [23].

Kada god se pojavio neki od virusa za iOS operativni sustav u kratkom vremenu je bio uklonjen i svakim pojavljivanjem Apple je uložio još više u svoju sigurnost i provjere kako se iste ne bi ponovile.

Tablica 6.2. Lista otkrivenih virusa za iOS operativni sustav

Naziv	Vrijeme otkrivanja	Pretpostavljeno podrijetlo	Tip
iOS/Toires.A!tr.spy	Studeni 2009.	Švicarska (Nicolas Seriot)	Dokaz koncepta
Adware/LBTM!iOS	Rujan 2010	Francuska	Pozivi prema Premium brojevima
iOS/FindCall.A!tr.spy	Srpanj 2012	Rusija	Trojan

Izvor: [28]

Navedene viruse nije bilo moguće instalirati na testiranom uređaju tvrtke Apple, iPhone 3GS-u.

5.6. Statistička analiza rezultata

Istraživanje se provelo na dva mobilna terminalna uređaja sa operativnim sustavima Android i iOS. Korišteno je pet antivirusnih alata, pet antivirusnih alata na Andorid mobilnom terminalnom uređaju i jedan na iOS mobilnom terminalnom uređaju.

Tablica 6.3. Statistička analiza dobivenih rezultata

Antivirusni alat	EICAR test	Analiza web stranica	Testiranje uzorcima malwarea
Lookout (Android)	+	100%	100%
Avast Mobile Security	+	*	100%
Trend Micro Mobile Security	+	92%	100%
McAfee Mobile Security	+	96%	100%
Norton Mobile Security	+	100%	100%
Lookout (iOS)	*	*	*

„+“ – označava uspješno obavljen test

„*“ - test nije moguće izvršiti

Kao što prikazuje Tablica 6.3. svi antivirusni alati sa Android operativnim sustavom su prepoznali EICAR datoteku te uzorke preuzetog *malwarea*. Oznaka „+“ u tablici označava da je antivirusni alat prepoznao EICAR test, a oznaka „*“ da nije bilo moguće obaviti testiranje jer funkcionalnost ne postoji ili nije moguće instalirati uzorak virusa na uređaj. Na iOS uređaj nije bilo moguće instalirati EICAR test jer ne postoji ista aplikacija na Apple Storeu. Rezultati analize web stranica i testiranje uzorcima malwarea prikazano je u postotcima, tako je na primjer Trend Micro Mobile Security antivirusni alat od 50 posjećenih stranica označio sigurnima njih 92% odnosno 46 stranica, 4 stranice odnosno 8 % su označene kao potencijalne prijetnje. Avast Mobile Security na Andorid operativnom sustavu i Lookout na iOS operativnom sustavu nisu imale mogućnost provjere web stranica prilikom pretraživanja. Također na iOS uređaj nije bilo moguće instalirati aplikacije treće strane jer uređaj nije bio *jailbreakan*[12] ili kako se još naziva otključan što ga ograničava na instaliranje aplikacija samo sa App Store-a.

Iz statističke analize se može zaključiti da su svi antivirusni alati pronašli potencijalne prijetnje sa visokim postotkom uspješnosti.

[12] Jailbreak – process uklanjanja ograničenja nametnutih od iOS-a, Apple-ovog operativnog sustava

7. Zaključak

Svakim danom broj mobilnih terminalnih uređaja se povećava, kao što je napomenuto ranije u radu 2014. godine broj terminalnih uređaja je premašio svjetsku populaciju. Rastom broja mobilnih terminalnih uređaja, raste i broj zlonamjernog sadržaja (*malwarea*), istraživanja tvrtke Pulse Secure procjenjuju da je u 2014. proizvedeno oko milijun novih virusa.

Iako se ovdje govori o velikom broju zlonamjernog sadržaja koji je u opticaju, možemo reći da su šanse „zaraze“ mobilnog terminalnog uređaja još uvijek male u odnosu na računala, što zbog same arhitekture operativnih sustava, načinu pokretanja aplikacija, a i samog broja zlonamjernog sadržaja.

Najviše zlonamjernog sadržaja može se pronaći u zemljama poput Rusije i Kine, zbog velikog broja korisnika mobilnih terminalnih uređaja te zbog neslužbenih trgovina sa aplikacijama za koje Google odnosno Apple na jamče sigurnost.

Android operativni sustav je više izložen zlonamjernom sadržaju od Apple operativnog sustava iOS, a jedan od razloga je jer čini oko 82.8 % operativnih sustava na tržištu mobilnih terminalnih uređaja prema istraživanju tvrtke IDC iz kolovoza 2015. godine. Također Android sustav je sustav otvorenog koda što ga čini ranjivijim od zatvorenog iOS-a. Android dopušta instaliranje aplikacija na tržištima treće strane dok to na iOS operativnom sustavu nije moguće osim ako se uređaj ne *jailbreak*-a, čime se ne jamči sigurnost podataka.

Istraživanje je pokazalo da prijetnje postoje, da pretraživanjem web stranica također možemo ugroziti sigurnost svog mobilnog terminalnog uređaja, ali postotak prijetnji je zanemariv ako se radi o posjećenijim svjetskim stranicama jer s obzirom na broj korisnika koji pristupaju takvim stranicama, vlasnici stranica se trude pružiti sigurnost korisnicima jer im je u interesu da broj posjetitelja i dalje raste.

Ukoliko se korisnici pridržavaju uputa proizvođača operativnih sustava, ne bi trebali imati problema sa zlonamjernim sadržajem jer je ipak razina provjere samih aplikacija na službenim trgovinama aplikacija, Google Play i App Store na visokoj razini.

Iako je vjerojatnost da će korisnik „zaraziti“ svoj mobilni terminalni uređaj vrlo mala, svakako se preporučuje instaliranje nekog od antivirusnih alata sa tržišta jer uvijek postoji mogućnost da se nađu u nekim nekontroliranim uvjetima kao što je spajanje na nepoznatu mrežu, dijeljenje podataka, pretraživanje nepoznatih stranica.

Kod odabira antivirusnog alata korisnicima se u najviše slučajeva nude besplatne i Premium verzije antivirusnih alata. Kod većine antivirusnih alata besplatna verzija je dostatna za osnovnu razinu sigurnosti. Razlike u antivirusnim alatima su male, a čak i „lošiji“ antivirusni alati pronalaze viruse u preko 95% posto slučajeva.

Potreba za antivirusnim alatima na mobilnim terminalnim uređajima još uvijek nije velika, ali u skorijoj budućnosti povećanjem broja samih mobilnih terminalnih uređaja, razvojem tehnologije i povećanjem korištenja Interneta stvari svakako će se pojaviti veća potreba za antivirusnim alatima.

Literatura

[1] Z. K. Miroslav Mikula, Terminalni uređaji u telekomunikacijskom prometu, Zagreb: Fakultet prometnih znanosti sveučilište u Zagrebu, 2000.

[2] C. n. c. emergency, »http://www.cert.hr/,« [Mrežno]. Available: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-303.pdf. [Pokušaj pristupa Srpanj 2015].

[3] S. Verma, »http://www.engineersgarage.com/,« Engineers Garage, [Mrežno]. Available: http://www.engineersgarage.com/invention-stories/mobile-phone-history. [Pokušaj pristupa Lipanj 2015].

[4] C. Baldwin, »http://www.computerweekly.com/,« Computer Weekly, Kolovoz 2012. [Mrežno]. Available: http://www.computerweekly.com/photostory/2240161527/Motorola-phones-through-the-ages/1/Motorola-DynaTAC-portable-cellular-telephone-prototype-circa-1973. [Pokušaj pristupa Lipanj 2015].

[5] J. Meyers, »http://www.businessinsider.com/,« Businessinsider, Svibanj 2011. [Mrežno]. Available: http://www.businessinsider.com/complete-visual-history-of-cell-phones-2011-5?op=1#ixzz3Ygyvzk22. [Pokušaj pristupa Lipanj 2015].

[6] »CBC Radio Canada,« CBC Radio Canada, Travanj 2013. [Mrežno]. Available: http://www.cbc.ca/news/technology/5-major-moments-in-cellphone-history-1.1407352. [Pokušaj pristupa Lipanj 2015].

[7] »Sharp world,« Sharp, [Mrežno]. Available: http://sharp-world.com/corporate/info/his/only_one/item/t34.html. [Pokušaj pristupa Srpanj 2015].

[8] »Gadgetizor,« Gadgetizor, Kolovoz 2010. [Mrežno]. Available: http://gadgetizor.com/sharp-j-sh04-worlds-first-ever-phone-with-integrated-camera-pictures-2001/5482/. [Pokušaj pristupa Lipanj 2015].

[9] »Radio-electronics,« Radio-electronics, [Mrežno]. Available: http://www.radio-electronics.com/info/cellulartelecomms/history/mobile-cell-phone.php. [Pokušaj pristupa Srpanj 2015].

[10] »Informatika Buzdo,« [Mrežno]. Available: http://www.informatika.buzdo.com/pojmovi/mobile-1.htm. [Pokušaj pristupa Kolovoz 2015].

[11] »Portal za poslovno e-ucenje,« [Mrežno]. Available: http://eucenje.efst.hr/category/o-poslovnom-e-ucenju/. [Pokušaj pristupa Lipanj 2015].

[12] »Cisco,« [Mrežno]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html. [Pokušaj pristupa Lipanj 2015].

[13] »Ericsson mobility report,« Ericsson, [Mrežno]. Available: http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-november-2014.pdf. [Pokušaj pristupa Svibanj 2015].

[14] »Centar informacijske sigurnosti,« [Mrežno]. Available: http://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-024.pdf. [Pokušaj pristupa Svibanj 2015].

[15] Q. Huang, »An extension to the Android,« Listopad 2011. [Mrežno]. Available: http://soda.swedish-ict.se/4207/1/MasterThesis_QingHuang.pdf. [Pokušaj pristupa Svibanj 2015].

[16] A. Inc., »iOS technology overview,« 2014. [Mrežno]. Available: https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iOSTechOverview.pdf. [Pokušaj pristupa Svibanj 2015].

[17] »Centar informacijske sigurnosti,« Rujan 2011. [Mrežno]. Available: http://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-024.pdf. [Pokušaj pristupa Lipanj 2015].

[18] »Lookout,« [Mrežno]. Available: https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat. [Pokušaj pristupa Lipanj 2015].

[19] C. McNutt, »Android Headlines,« [Mrežno]. Available: http://www.androidheadlines.com/2015/01/newest-version-avast-mobile-security-now-available.html. [Pokušaj pristupa Kolovoz 2015].

[20] C. C. Systems, »CS Computer Systems,« [Mrežno]. Available: http://www.cs.hr/trend-micro.asp. [Pokušaj pristupa Rujan 2015].

[21] »GSMAren,« [Mrežno]. Available: http://www.gsmarena.com/compare.php3?idPhone1=3468&idPhone2=2826. [Pokušaj pristupa Rujan 2015].

[22] E. Willems, »The winds of change: Up-Dates to the EICAR test file,« *Virus Bulletin,* 2003.

[23] J. Kirk, IDG News Service, [Mrežno]. Available: http://www.pcworld.com/article/2844292/apple-mobile-devices-in-china-targeted-by-wirelurker-malware.html. [Pokušaj pristupa Rujan 2015].

[24] »Avast,« Avast , [Mrežno]. Available: https://www.avast.com/about. [Pokušaj pristupa Srpanj 2015].

[25] »Trend Micro,« [Mrežno]. Available: http://eeur.trendmicro.eu/. [Pokušaj pristupa Kolovoz 2015].

[26] Mcafee, Mcafee, [Mrežno]. Available: http://home.mcafee.com/. [Pokušaj pristupa Rujan 2015].

[27] M. Riofrio, pcworld, [Mrežno]. Available: http://www.pcworld.com/article/2042963/new-norton-mobile-security-includes-database-of-4-million-scanned-android-apps.html. [Pokušaj pristupa Rujan 2015].

[28] A. Apvrille, Fortinet, Lipanj 2014. [Mrežno]. Available: https://blog.fortinet.com/post/ios-malware-does-exist. [Pokušaj pristupa Rujan 2015].

Popis slika

Slika 2.1. a) Motorola DynaTAC, [4] b) Motorola MicroTA, [5] C c) IBM Simon, [6] 3
Slika 2.2. Sharp J-SH04 i fotografija snimljen njegovom kamerom, [7], [8] 4
Slika 2.3. Motorola RAZR, [5] 5
Slika 2.4. Apple iPhone, [5] 5
Slika 2.5. HTC Dream, [5] 5
Slika 2.6. HTC EVO 4G, [5] 6
Slika 3.1. Arhitektura Android operativnog sustava, [10] 11
Slika 3.2. Implementacija iOS tehnologije, [16] 12
Slika 5.1. Sučelje Lookout aplikacije 18
Slika 5.2. Podizbornik izbornika Backup 19
Slika 5.3. Prediktivna sigurnost, [18] 20
Slika 5.4. Savjetnik za privatnost, [18] 20
Slika 5.5. Sigurno pretraživanje, [18] 21
Slika 5.6. Lociranje i zvučno upozorenje, [18] 21
Slika 5.7. Odbljesak signala, [18] 22
Slika 5.8. Upozorenje o krađi, [18] 22
Slika 5.9. Zaključavanje uređaja, [18] 23
Slika 5.10. Sigurnosno kopiranje podataka, [18] 23
Slika 5.11. Skeniranje virusa 25
Slika 5.12. Wi-Fi sigurnost 26
Slika 5.13. Zaključavanje aplikacija 26
Slika 5.14. Savjetnik za sigurnost 27
Slika 5.15. Upravljanje aplikacijama 27
Slika 5.16. Filter poziva i SMS-ova 28
Slika 5.17. Mjerač prometa 28
Slika 5.18. Sučelje Trend Micro aplikacije 31
Slika 5.19. Podizbornik skeniranja virusa 32
Slika 5.20. Podizbornik skenera privatnosti 33
Slika 5.21. Podizbornik sigurnog surfanja i roditeljske zaštite 33
Slika 5.22. Podizbornik blokiranja poziva i poruka 34
Slika 5.23. Podizbornik zaštite izgubljenog uređaja 35
Slika 5.24. Podizbornici skeniranja Facebooka-a i optimiziranje baterije i memorije uređaja 35
Slika 5.25. Skeniranje u Trend Micro aplikaciji 36
Slika 5.26. Početni zaslon McAfee aplikacije 37
Slika 5.27. Podizbornik sigurnosnog pregleda 38
Slika 5.28. Podizbornik privatnosti 39
Slika 5.29. Podizbornik optimiziranja baterije 40
Slika 5.30. Podizbornik traženja uređaja 40

Slika 5.31. Podizbornik sigurnosnog kopiranja 41
Slika 5.32. Podizbornik sigurnosnog pregleda 42
Slika 5.33. Izbornik Norton Mobile Security-a 43
Slika 5.34. Podizbornik Anti-Malware 44
Slika 5.35. Anti-Theft funkcionalnost 45
Slika 5.36. Podizbornik Backup-a 45
Slika 5.37. Podizbornik Call Blockinga 46
Slika 5.38. Podizbornik Web zaštite 46
Slika 6.1. HTC Desire HD uređaj 48
Slika 6.2. Specifikacije HTC Desire HD uređaja, [21] 48
Slika 6.3. Apple iPhone 3GS 49
Slika 6.4. Specifikacije Apple iPhone 3GS-a 49
Slika 6.5. Lookout, Avast i McAfee prepoznaju EICAR datoteku kao malware 50
Slika 6.6. Trend Micro Mobile Security i Norton Mobile Security prepoznaju EICAR datoteku kao malware 51
Slika 6.8. Izvješće o sigurnosti web stranica pojedinih antivirusnih alata 52
Slika 6.9. Lookout prepoznaje instalirani malware 54
Slika 6.10. Avast prepoznaje instalirani malware 54
Slika 6.11. Trend Micro prepoznaje instalirani malware 55
Slika 6.12. McAfee prepoznaje instalirani malware 55
Slika 6.13. Norton prepoznaje instalirani malware 56

Popis tablica

Tablica 2.1.Prodaja mobilnih uređaja u odnosu na PC i tablet uređaje 8
Tablica 2.2. Broj mobilnih terminalnih uređaja 8
Tablica 5.1. Usporedba funkcionalnosti besplatne i Premium verzije Lookout aplikacije 17
Tablica 5.2.Usporedba funkcionalnosti besplatne i Premium verzije Trend Micro aplikacije 30
Tablica 6.1. 50 najposjećenijih web stranica u Hrvatskoj 52
Tablica 6.2. Lista otkrivenih virusa za iOS operativni sustav 57
Tablica 6.3. Statistička analiza dobivenih rezultata 57